Symantec pcAnywhere™ Administratorhandbuch

Symantec pcAnywhere Administratorhandbuch

Die im vorliegenden Handbuch beschriebene Software unterliegt einem Lizenzvertrag und kann ausschließlich in Übereinstimmung mit den Bestimmungen dieses Vertrags verwendet werden.

Dokumentation Version 11.0

Teilenr.: 10092987-GE

Copyright

Copyright © 2003 Symantec Corporation.

Alle Rechte vorbehalten.

Jedes von der Symantec Corporation bereitgestellte technische Dokument ist als Eigentum der Symantec Corporation urheberrechtlich geschützt.

KEINE GARANTIE. Die technische Dokumentation wird Ihnen WIE VORGELEGT zur Verfügung gestellt, und die Symantec Corporation übernimmt keine Gewährleistung bezüglich der Genauigkeit oder Nutzung dieser Dokumentation. Jegliche Verwendung der technischen Dokumentation oder der darin enthaltenen Informationen durch den Benutzer erfolgt auf eigene Gefahr. Es ist möglich, dass die Dokumentation technische oder andere Ungenauigkeiten bzw. typografische Fehler enthält. Symantec behält sich das Recht auf Änderungen ohne Vorankündigung vor.

Das Kopieren dieser Dokumentation im Ganzen oder in Auszügen bedarf der vorherigen schriftlichen Genehmigung durch die Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, USA.

Marken

In den USA sind das Symantec-Logo, Symantec pcAnywhere, ColorScale und SpeedSend eingetragene Marken der Symantec Corporation. Symantec Packager und LiveUpdate sind Marken der Symantec Corporation.

Andere Marken und Produktnamen, die in diesem Handbuch erwähnt werden, können Marken oder eingetragene Marken ihrer Eigentümer sein und werden hiermit als solche anerkannt.

Gedruckt in Irland.

10 9 8 7 6 5 4 3 2 1

Inhaltsverzeichnis

Kapitel 1 Vorbereitung der Installation von Symantec pcAnywhere

Vorbereitung der Installation 8
- Systemanforderungen 8
- Erforderliche Benutzerrechte 9
- Installationsoption auswählen 10
- Wenn eine vorherige Version installiert ist 11

Planen einer Migrations- und Aktualisierungsstrategie 12
- Von pcAnywhere 10.x unter Windows NT/2000/XP migrieren 13
- Von pcAnywhere 10.x unter Windows 98/Me migrieren 14
- AutoTransfer-Dateien konvertieren 14
- Von pcAnywhere 9.2x unter Windows NT/2000/XP aktualisieren 15
- Von pcAnywhere 9.2x unter Windows 98/Me aktualisieren 15

Optimieren von Migrationen und Aktualisierungen mit
- Symantec Packager 16

Kapitel 2 Erstellen angepasster Installationspakete

Wissenswertes zu Symantec Packager 18
Verwendung von Symantec Packager 18
Funktionsweise von Symantec Packager 19
Importieren eines Produktmoduls 21
Anpassen der Produkteinstellungen 22
- Produktfunktionen auswählen 23
- Konfigurationsdateien einbinden 25
- Integritätsprüfung einer Produktkonfiguration 29
- pcAnywhere-Installation eine Seriennummer zuweisen 30
- Konfigurationseinstellungen global verwalten 33
- Produktinstallationsoptionen festlegen 36

Erstellen eines benutzerdefinierten Befehls 43
Erstellen von Installationspaketen 44
- Produkte und Befehle zu einer Paketdefinition hinzufügen 45

Generieren von Produktinstallationen und Paketen 46
- Produktkonfigurationsdatei generieren 46
- Paket generieren 47

Testen von Paketen 48

Kapitel 3 Verteilen angepasster Installationen von Symantec pcAnywhere

Informationen zur Verteilung 50
Informationen zu den Installationsdateiverzeichnissen 51
Verteilen von Installationspaketen mit Hilfe der webbasierten Verteilung 51
Anforderungen für die webbasierte Verteilung 52
Installations-Web-Server einrichten 52
Verteilungsdateien anpassen 56
Installation testen 60
Benutzer über den Speicherort zum Herunterladen informieren 60
Verteilen von pcAnywhere mit Hilfe von SMS 2.0 61
Mindestanforderungen für die SMS-Installation 61
pcAnywhere mit SMS verteilen 62
Windows NT/2000/XP-Anmeldeskripts 65
Server einrichten 65
Anmeldeskript erstellen 66
Anmeldeskript testen 67
NetWare-Anmeldeskripts 67
Server einrichten 67
Anmeldeskript erstellen 68
Anmeldeskript testen 69

Kapitel 4 Zentrales Management

Informationen zum zentralen Management 72
Fernverwaltung von pcAnywhere-Hosts 72
pcAnywhere Host-Administrator-Tool installieren 72
Host-Administrator-Snap-In zu MMC hinzufügen 74
Konfigurationsgruppen erstellen 74
Computer zu einer Konfigurationsgruppe hinzufügen 75
Administrator-Host- und Remote-Verbindungsobjekte konfigurieren 76
Host-Objekt im pcAnywhere Host-Administrator konfigurieren 79
pcAnywhere-Konfigurationsdateien verteilen 79
Hosts in einer Konfigurationsgruppe verwalten 80
Integration in Microsoft Systems Management Server (SMS) 81
Paketdefinitionsdatei in SMS importieren 81

Informationen zu Microsoft Distributed Component Object Model (DCOM) ... 82
Windows NT/2000/XP für DCOM konfigurieren ... 82
Windows 98/Me für DCOM konfigurieren ... 83
DCOM-Einstellungen bearbeiten ... 83
AwShim ... 84
Informationen zur zentralen Protokollierung ... 85
Leistung mit Hilfe von SNMP-Traps überwachen ... 85
pcAnywhere MIB-Datei ... 86

Kapitel 5 Integrieren von pcAnywhere in Verzeichnisdienste

Verzeichnisdienste ... 118
Überblick über das LDAP Informational Model ... 118
Verzeichnisdienste und pcAnywhere ... 120
Konfigurieren der Verzeichnisserver ... 120
LDAP-Server konfigurieren ... 120
Netscape Directory Server 3.1 konfigurieren ... 121
Netscape Directory Server 4.0 konfigurieren ... 122
Novell 5.0-Server konfigurieren ... 123
Windows Active Directory konfigurieren ... 128
Konfigurieren von pcAnywhere für die Verwendung von Verzeichnisdiensten ... 133
Verzeichnisdienste in pcAnywhere einrichten ... 133
Host-Computer für die Verwendung von Verzeichnisdiensten einrichten ... 134
Remote-Computer für die Verwendung von Verzeichnisdiensten einrichten ... 135

Kapitel 6 Sicherheit in Symantec pcAnywhere

Methoden zum Sichern von pcAnywhere ... 138
pcAnywhere und Windows-Sicherheit ... 138
Kontrolle des Zugriffs auf pcAnywhere-Hosts ... 139
Verbindungen nur für bestimmte Computernamen oder IP-Adressen zulassen ... 140
Zentrale Authentifizierung in pcAnywhere nutzen ... 141
Sichern der Sitzungen ... 147
Überwachen von Sitzungen ... 148
Konfigurieren einer richtliniengestützten Verwaltung ... 149
Gruppenrichtlinien in Windows 2000/XP konfigurieren ... 149
Systemrichtlinien in Windows 98/Me/NT4 konfigurieren ... 149
pcAnywhere-Verwaltungsvorlagen importieren ... 150
Benutzerrichtlinien verwalten ... 152

Kapitel 7 Erkennen von Sicherheitsrisiken

Informationen zum Remote Access Perimeter Scanner 158
Haftungsausschluss 158
Überprüfte Produkte 159
Installieren des Remote Access Perimeter Scanner 160
Öffnen des Remote Access Perimeter Scanner 161
Remote Access Perimeter Scanner in der Befehlszeile ausführen 162
Einstellen von globalen Optionen 162
Protokollieren von Remote Access Perimeter Scanner-Ereignissen 164
Ereignisprotokollklassifikationen 164
SNMP-Traps einstellen 165
Windows-Ereignisprotokollierung einrichten 166
Erstellen einer angepassten Prüfdatei 167
Prüfdatei erstellen und speichern 167
Befehle zu einer Prüfdatei hinzufügen 168
Befehle ändern 176
Befehle aus einer Prüfdatei löschen 176
Ausführen einer Remote Access Perimeter Scanner-Prüfung 176
Anzeigen von Prüfergebnissen 177

Index

Lösungen für Service und Unterstützung

Kapitel 1

Vorbereitung der Installation von Symantec pcAnywhere

In diesem Kapitel werden folgende Themen behandelt:

- Vorbereitung der Installation
- Planen einer Migrations- und Aktualisierungsstrategie
- Optimieren von Migrationen und Aktualisierungen mit Symantec Packager

Vorbereitung der Installation

Vergewissern Sie sich vor der Installation von pcAnywhere, dass Ihr Computer die Systemanforderungen erfüllt. Lesen Sie die Readme-Datei auf der Installations-CD, um sich über bekannte Probleme zu informieren.

Informationen zur Installation finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Hinweis: Die Installation von Symantec pcAnywhere auf verschlüsselten Dateisystemen wird nicht unterstützt.

Systemanforderungen

Symantec pcAnywhere kann unter Windows 98/Me/NT/2000/XP installiert werden. Damit das Programm ordnungsgemäß ausgeführt wird, müssen mindestens die in Tabelle 1-1 aufgeführten Ressourcen auf Ihrem System vorhanden sein.

Tabelle 1-1 Systemanforderungen

Betriebssystem	Anforderungen
Windows XP Home Edition/Professional	■ Service Pack ab Version 1 (SP1) ■ Intel Pentium-Prozessor (oder kompatibler Prozessor) ab 233 MHz ■ 64 MB RAM (128 MB empfohlen) ■ 32 MB freier Festplattenspeicher ■ VGA-Grafikmonitor oder höhere Auflösung ■ CD-ROM- oder DVD-Laufwerk
Windows 2000 Professional/Server	■ Service Pack ab Version 3 (SP3) ■ Intel Pentium-Prozessor (oder kompatibler Prozessor) ab 150 MHz ■ 64 MB Arbeitsspeicher ■ 32 MB freier Festplattenspeicher ■ VGA-Grafikmonitor oder höhere Auflösung ■ CD-ROM- oder DVD-Laufwerk

Tabelle 1-1 Systemanforderungen

Betriebssystem	Anforderungen
Windows NT Workstation 4/NT Server 4	■ Service Pack ab Version 6 (SP6) ■ Intel Pentium-Prozessor (oder kompatibler Prozessor) ab 150 MHz ■ 64 MB Arbeitsspeicher ■ 32 MB freier Festplattenspeicher ■ VGA-Grafikmonitor oder höhere Auflösung ■ CD-ROM- oder DVD-Laufwerk
Windows 98/Me	■ Intel Pentium-Prozessor (oder kompatibler Prozessor) ab 150 MHz ■ 64 MB Arbeitsspeicher ■ 32 MB freier Festplattenspeicher ■ VGA-Grafikmonitor oder höhere Auflösung ■ CD-ROM- oder DVD-Laufwerk

Darüber hinaus sind die folgenden Programme von Fremdherstellern erforderlich, um die ordnungsgemäße Ausführung bestimmter Funktionen sicherzustellen. Diese Programme befinden sich auf der pcAnywhere Installations-CD im Ordner "Tools".

- Adobe Acrobat Reader ab Version 5.1
- Internet Explorer ab Version 5.5 SP2

Erforderliche Benutzerrechte

Benutzer unter Windows NT/2000/XP benötigen Administratorrechte, um pcAnywhere zu installieren.

Windows XP lässt nicht zu, dass Benutzer, die den eingeschränkten Benutzerkonten oder Gastkonten zugewiesen wurden, Software installieren oder deinstallieren, systemweit geltende Einstellungen ändern oder Benutzerkonten hinzufügen, bearbeiten bzw. löschen. Melden Sie sich bei der Ausführung von pcAnywhere unter Windows XP als Benutzer mit Administratorrechten an, um eine optimale Leistung zu erzielen.

Installationsoption auswählen

Symantec pcAnywhere ermöglicht eine vollständige oder benutzerdefinierte Installation. Bei der benutzerdefinierten Installation werden nur die Funktionen installiert, die Sie benötigen. In Tabelle 1-2 sind die verfügbaren Installationsoptionen aufgeführt.

Tabelle 1-2 Installationsoptionen

Installationsoption	Beschreibung
Symantec pcAnywhere	Installiert die Vollversion von pcAnywhere, einschließlich Host, Fernsteuerung, Fernverwaltung und Dateiübertragung. Bei der Corporate-CD enthält diese Installation auch das Host-Administrator-Tool und den Remote Access Perimeter Scanner. Bei der CD, die im Einzelhandel erhältlich ist, enthält diese Installation auch das Host-Administrator-Tool.
pcAnywhere für Einzelbenutzer	Installiert die Vollversion von pcAnywhere ohne das Host-Administrator-Tool oder den Remote Access Perimeter Scanner.
Nur Host-Version	Installiert Host-Server-Funktionen, wobei Netzwerk- und Modemverbindungen unterstützt werden. Wählen Sie diese Option, wenn Sie nur Verbindungen empfangen möchten, oder wenn Sie pcAnywhere auf zwei Computern installieren möchten, wobei ein Computer ein Host- und der andere Computer ein Remote-Computer ist.
LAN Host-Version	Installiert Host-Server-Funktionen, wobei nur Netzwerkverbindungen unterstützt werden. Wählen Sie diese Option, wenn Sie nur Verbindungen empfangen möchten, oder wenn Sie pcAnywhere auf zwei Computern installieren möchten, wobei ein Computer ein Host- und der andere Computer ein Remote-Computer ist.
Nur Remote-Version	Installiert die Funktionen zum Herstellen einer Verbindung mit einem Host-Computer für Fernsteuerung, Fernverwaltung und Dateiübertragung. Die Host-Server-Funktionen sind nicht eingeschlossen. Wählen Sie diese Option, wenn Sie nur Verbindungen starten möchten, oder wenn Sie pcAnywhere auf zwei Computern installieren möchten, wobei ein Computer ein Host- und der andere Computer ein Remote-Computer ist.

Tabelle 1-2 Installationsoptionen

Installationsoption	Beschreibung
pcAnywhere Express	Mit Hilfe von pcAnywhere Express können Sie eine Verbindung zu einem anderen Computer über einen beliebigen Web-Browser herstellen, der ActiveX-Steuerelemente unterstützt. Für diese Installationsoption wird keine technische Unterstützung bereitgestellt.
pcAnywhere mit DynIP	Installiert ein benutzerdefiniertes Paket, in dem die Vollversion von pcAnywhere zusammen mit einer sechsmonatigen Testversion von DynIP enthalten ist. Für diese Installationsoption wird keine technische Unterstützung bereitgestellt.

Wenn eine vorherige Version installiert ist

Während der Installation sucht pcAnywhere automatisch nach einer bereits vorhandenen Version. Wenn Sie pcAnywhere auf einem Computer installieren, auf dem bereits pcAnywhere ab Version 10.0x installiert ist, werden Sie aufgefordert anzugeben, ob bestehende Daten beibehalten werden sollen, bevor die vorherige Version überschrieben wird. Die Handhabung der Datenkonvertierung durch pcAnywhere hängt vom Betriebssystem und der installierten pcAnywhere-Version ab.

Siehe "Planen einer Migrations- und Aktualisierungsstrategie" auf Seite 12.

Wenn Sie pcAnywhere auf einem Computer installieren, auf dem bereits pcAnywhere 9.2.1 oder früher installiert ist, werden Sie zum Deinstallieren dieser Version aufgefordert. Dabei werden alle bestehenden Konfigurationsdaten entfernt. Die Konfigurationsdaten dieser Versionen können nicht konvertiert oder beibehalten werden. Falls Sie die neue Version auf mehreren Computern installieren möchten, auf denen eine nicht unterstützte Version von pcAnywhere installiert ist, können Sie den Installationsvorgang mit Symantec Packager vereinfachen.

Siehe "Optimieren von Migrationen und Aktualisierungen mit Symantec Packager" auf Seite 16.

Planen einer Migrations- und Aktualisierungsstrategie

Symantec pcAnywhere unterstützt die Migration von Version 10.x nach Version 11.0 unter Windows 98/Me/NT/2000/XP. Während der Migration gestattet pcAnywhere das Installieren über eine vorherige Produktversion und das Beibehalten benutzerdefinierter Einstellungen.

Symantec pcAnywhere unterstützt Aktualisierungen von Version 9.2x nach Version 11.0 unter Windows 98/Me/NT/2000/XP. Bei einer Aktualisierung kann über die vorherige Produktversion installiert werden. Benutzerdefinierte Einstellungen werden jedoch nicht automatisch beibehalten.

Ein Neustart des Systems ist für Migrationen und Aktualisierungen nur dann erforderlich, wenn Systemdateien aktualisiert werden müssen. Nach der Installation von Symantec pcAnywhere ist ein Systemneustart erforderlich, wenn Sie unter Windows 98/Me auf die neue Version umstellen oder aktualisieren.

Symantec Packager vereinfacht die Deinstallation früherer Versionen oder die Verteilung von vorkonfigurierten Einstellungen an mehrere Benutzer.

Siehe "Optimieren von Migrationen und Aktualisierungen mit Symantec Packager" auf Seite 16.

Nehmen Sie die in Tabelle 1-3 aufgeführten Informationen bei der Planung der Migrations- und Aktualisierungsstrategie zur Hilfe.

Tabelle 1-3 Übersicht über die Migrations- und Aktualisierungsstrategie für Symantec pcAnywhere

Symantec pcAnywhere-Version	Betriebssystem	Neustart erforderlich	Daten werden automatisch beibehalten
10.x	Windows NT/ 2000/XP	Nein	Host-Objekte Anruferobjekte Remote-Objekte Optionsgruppen Registrierungseinstellungen AutoTransfer-Dateien (Konvertierung erforderlich)

Tabelle 1-3 Übersicht über die Migrations- und Aktualisierungsstrategie für Symantec pcAnywhere

Symantec pcAnywhere-Version	Betriebssystem	Neustart erforderlich	Daten werden automatisch beibehalten
10.x	Windows 98/Me	Ja	Host-Objekte Anruferobjekte Remote-Objekte Optionsgruppen Registrierungseinstellungen AutoTransfer-Dateien (Konvertierung erforderlich)
9.2x	Windows NT/ 2000/XP	Nein	Keine
9.2x	Windows 98/Me	Ja, vorherige Version muss deinstalliert werden	Keine

Von pcAnywhere 10.x unter Windows NT/2000/XP migrieren

Symantec pcAnywhere unterstützt die vollständige Migration ohne Neustart des Systems, wenn pcAnywhere 11.0 auf einem Computer unter Windows NT/2000/XP installiert wird, auf dem die folgenden Versionen von pcAnywhere 10.x installiert sind.

- Vollversion des Produkts
- Nur Host-Version

Während der Installation werden Sie gefragt, ob bestehende Konfigurationseinstellungen beibehalten werden sollen. Dazu zählen Einstellungen für Host-, Remote- und Anruferobjekte sowie Optionsgruppen.

AutoTransfer-Dateien (.atf), die in früheren Versionen von pcAnywhere erstellt wurden, werden beibehalten. Damit Sie die .atf-Dateien jedoch in dieser pcAnywhere-Version verwenden können, müssen Sie sie in Befehlswarteschlangendateien konvertieren.

Siehe "AutoTransfer-Dateien konvertieren" auf Seite 14.

Die Migration von reinen Remote-Paketen und integritätsgeprüften Paketen wird nicht unterstützt.

Von pcAnywhere 10.x unter Windows 98/Me migrieren

Symantec pcAnywhere unterstützt die vollständige Migration, wenn pcAnywhere 11.0 auf einem Computer unter Windows 98/Me installiert wird, auf dem die folgenden Versionen von pcAnywhere 10.x installiert sind.

- Vollversion des Produkts
- Nur Host-Version

Während der Installation werden Sie gefragt, ob bestehende Konfigurationseinstellungen beibehalten werden sollen. Dazu zählen Einstellungen für Host-, Remote- und Anruferobjekte sowie Optionsgruppen.

AutoTransfer-Dateien (.atf), die in früheren Versionen von pcAnywhere erstellt wurden, werden beibehalten. Damit Sie die .atf-Dateien jedoch in dieser pcAnywhere-Version verwenden können, müssen Sie sie in Befehlswarteschlangendateien konvertieren.

Siehe "AutoTransfer-Dateien konvertieren" auf Seite 14.

Bei dieser Migration ist ein Neustart des Systems erforderlich, um ältere pcAnywhere-Systemdateien zu entfernen. Sie können den Migrationsprozess mit Hilfe von Symantec Packager rationalisieren.

Siehe "Optimieren von Migrationen und Aktualisierungen mit Symantec Packager" auf Seite 16.

Die Migration von reinen Remote-Paketen und integritätsgeprüften Paketen wird nicht unterstützt.

AutoTransfer-Dateien konvertieren

Die Befehlswarteschlange ersetzt in der neuen Version von Symantec pcAnywhere die AutoTransfer-Funktion, die in früheren pcAnywhere-Versionen vorhanden war. Bei der Migration von pcAnywhere 10.x auf pcAnywhere 11.0 übernimmt pcAnywhere die AutoTransfer-Dateien (.atf), die im pcAnywhere-Standardprogrammverzeichnis gespeichert sind, in die neue Version. Um diese Dateien jedoch in pcAnywhere 11.0 nutzen zu können, müssen Sie sie in Befehlswarteschlangendateien konvertieren.

Symantec pcAnywhere stellt ein ATF Converter-Programm bereit, mit dem Sie in pcAnywhere 10.0 (oder mit einer früheren Version) erstellte .atf-Dateien in Befehlswarteschlangendateien konvertieren können. Das ATF Converter-Programm ist im Ordner "Unsupported" auf der Symantec pcAnywhere-CD gespeichert.

Von pcAnywhere 9.2x unter Windows NT/2000/XP aktualisieren

Symantec pcAnywhere unterstützt unter Windows NT/2000/XP Aktualisierungen von vollständigen Produktversionen und Nur-Host-Versionen von pcAnywhere 9.2x auf Version 11.0. Das System muss nicht neu gestartet werden.

Beim Aktualisierungsvorgang werden benutzerdefinierte Daten nicht automatisch beibehalten. Falls Sie pcAnywhere auf mehreren Computern aktualisieren möchten, können Sie mit Symantec Packager ein benutzerdefiniertes Installationspaket erstellen, das vorkonfigurierte Datendateien enthält.

Siehe "Optimieren von Migrationen und Aktualisierungen mit Symantec Packager" auf Seite 16.

Von pcAnywhere 9.2x unter Windows 98/Me aktualisieren

Wenn Sie pcAnywhere 11.0 auf einem Computer unter Windows 98/Me installieren, auf dem bereits Version 9.2x installiert ist, werden Sie von pcAnywhere zum Deinstallieren des Programms aufgefordert. Dies ist notwendig, um den fehlerfreien Betrieb sicherzustellen.

Sie können diesen Vorgang automatisieren und mit Symantec Packager ein benutzerdefiniertes Installationspaket erstellen, das den Deinstallations- und Installationsvorgang übernimmt. Sie können auch vorkonfigurierte Datendateien zu dem Paket hinzufügen und das Paket an andere Benutzer verteilen.

Siehe "Optimieren von Migrationen und Aktualisierungen mit Symantec Packager" auf Seite 16.

Optimieren von Migrationen und Aktualisierungen mit Symantec Packager

Symantec Packager ist ein Administrator-Tool, mit dem Sie angepasste Installationspakete erstellen, bearbeiten und zusammenstellen können, um sie an andere Systeme zu verteilen. Symantec Packager ist als Installationsoption auf der pcAnywhere-CD verfügbar.

Symantec Packager unterstützt Sie wie folgt bei der Migration oder Aktualisierung von früheren pcAnywhere-Versionen:

Für die Produktinstallation müssen Sie manuell eine frühere Version des Produkts deinstallieren.	Erstellen Sie ein benutzerdefiniertes Installationspaket, und fügen Sie die Befehle hinzu, mit denen eine frühere Version ohne Benutzerabfragen vor der Installation des Produkts deinstalliert wird.
Nach der Produktinstallation ist ein Neustart des Computers erforderlich, um den Installationsprozess abzuschließen.	Erstellen Sie ein benutzerdefiniertes Installationspaket für die Produktinstallation, und konfigurieren Sie das Paket so, dass die Installation im passiven oder "Ohne Ausgabe"-Modus ausgeführt wird.
Bei der Produktinstallation werden keine vorkonfigurierten Produkteinstellungen beibehalten.	Erstellen Sie ein benutzerdefiniertes Installationspaket, und fügen Sie vorkonfigurierte Datendateien mit den von Ihnen benötigten Einstellungen hinzu.

Siehe "Erstellen angepasster Installationspakete" auf Seite 17.

Kapitel 2

Erstellen angepasster Installationspakete

In diesem Kapitel werden folgende Themen behandelt:

- Wissenswertes zu Symantec Packager
- Verwendung von Symantec Packager
- Funktionsweise von Symantec Packager
- Importieren eines Produktmoduls
- Anpassen der Produkteinstellungen
- Erstellen eines benutzerdefinierten Befehls
- Erstellen von Installationspaketen
- Generieren von Produktinstallationen und Paketen
- Testen von Paketen

Wissenswertes zu Symantec Packager

Mit Symantec Packager können Sie angepasste Installationspakete erstellen, bearbeiten und zusammenstellen, um sie an andere Systeme zu verteilen. Auf diese Weise können Sie Installationen gezielt an die Anforderungen Ihres Unternehmens anpassen und Pakete erstellen, die nur diejenigen Funktionen und Einstellungen enthalten, die Ihre Benutzer benötigen.

In Installationspaketen enthaltene Symantec-Produkte sind durch Copyright-Gesetze und die Symantec-Lizenzvereinbarung geschützt. Für die Verteilung von Paketen wird für jeden Benutzer, der das Paket installiert, eine Lizenz benötigt.

Hinweis: Symantec Packager läuft nur unter Windows NT/2000/XP Professional. Mit Symantec Packager erstellte Installationspakete können jedoch auch auf jeder Microsoft 32-Bit-Plattform mit Ausnahme von Windows 95 und Windows NT 3.51 installiert werden.

Verwendung von Symantec Packager

Mit Symantec Packager können Sie folgende Aufgaben ausführen:

- Produkte an die Sicherheitsrichtlinien Ihres Unternehmens anpassen, indem Sie Benutzern Zugriff auf alle verfügbaren Funktionen gewähren oder den Zugriff entsprechend einschränken.
- Netzwerkbelastung bei der Verteilung und Umfang der Anwendung durch ein angepasstes Installationspaket reduzieren, das nur die von den Benutzern benötigten Funktionen enthält.
- Komplexität der Installation mit Hilfe von vorkonfigurierten Datendateien verringern.
- Reduzieren der Verteilungskosten und Vereinfachen des Installationsvorgangs durch die gleichzeitige Installation mehrerer Produkte.
- Vereinfachen der Verteilung und Migration der Anwendung, indem benutzerdefinierte Befehle in Paketinstallationen aufgenommen werden.

Funktionsweise von Symantec Packager

Symantec Packager arbeitet bei der Erstellung von benutzerdefinierten Installationspaketen mit einem Prozess, der sich aus mehreren Phasen zusammensetzt. Jede Phase hängt von der Ausgabe der vorherigen Phase ab.

Abbildung 2-1 Übersicht über die Symantec Packager-Phasen

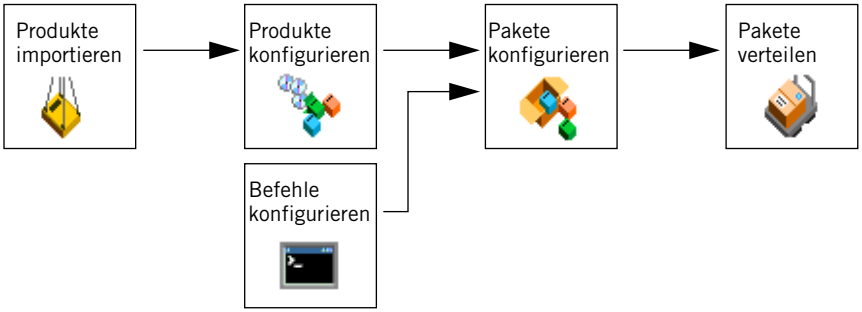


Abbildung 2-1 zeigt den Vorgang zum Erstellen benutzerdefinierter Installationspakete mit Symantec Packager. Folgende Schritte müssen ausgeführt werden:

- Produktmodule in Symantec Packager importieren

  Produktmodule enthalten die Installationsprogrammdateien und die Produktvorlagendateien, die zum Erstellen angepasster Installationen des Produkts erforderlich sind.

  Siehe "Importieren eines Produktmoduls" auf Seite 21.

- Produkte konfigurieren

  Für jedes Produkt können Sie die für die Benutzer verfügbaren Funktionen auswählen, vorkonfigurierte Daten und Konfigurationsdateien hinzufügen und Standardinstallationsoptionen einstellen.

  Siehe "Anpassen der Produkteinstellungen" auf Seite 22.

- Befehle für ein Paket konfigurieren

  Mit Hilfe benutzerdefinierter Befehle können Sie zusätzliche Funktionen hinzufügen, die in den Produktvorlagen nicht unterstützt werden. Beispielsweise können Sie ein Programm eines Fremdherstellers oder eine Stapeldatei hinzufügen.

  Siehe "Erstellen eines benutzerdefinierten Befehls" auf Seite 43.

- Pakete konfigurieren

  Fassen Sie eine oder mehrere Produktkonfigurationen und benutzerdefinierte Befehle zu einem Paket zusammen. Darüber hinaus können Sie das Paket weiter anpassen, indem Sie Installationsoptionen, die Reihenfolge der Produktinstallationen und andere Einstellungen für das Paket festlegen.

  Siehe "Erstellen von Installationspaketen" auf Seite 44.

- Benutzerdefinierte Produkte oder Pakete generieren

  Wenn Sie ein Paket generieren, legt Symantec Packager eine Installationsdatei an, die das Produkt, den Befehl und die von Ihnen festgelegten Paketoptionen enthält.

  Mit Symantec Packager können Sie aber auch eine Produktkonfigurationsdatei erstellen. Dabei wird eine Microsoft Installer-Datei (.msi) für eine Einzelproduktinstallation erstellt.

  Siehe "Generieren von Produktinstallationen und Paketen" auf Seite 46.

- Paket testen

  Testen Sie die Pakete vor dem Verteilen an die Endanwender, um die ordnungsgemäße Funktionalität sicherzustellen.

  Siehe "Testen von Paketen" auf Seite 48.

- Paket verteilen

  Auf der Registerkarte "Pakete verteilen" werden die von Ihnen erstellten Pakete angezeigt, die Sie an die Benutzer verteilen können. Symantec stellt ein Paketverteilungs-Tool in Symantec Packager und ein webbasiertes Verteilungs-Tool auf der pcAnywhere-CD bereit. Sie können aber auch Ihre eigenen Verteilungs-Tools verwenden.

  Siehe "Verteilen angepasster Installationen von Symantec pcAnywhere" auf Seite 49.

Importieren eines Produktmoduls

Produktmodule sind die Bausteine für das Erstellen von Paketen. Symantec Packager extrahiert die Produktvorlage und die Binärdateien der Produktinstallation aus dem Produktmodul. Die Produktvorlage beschreibt die Funktionsanforderungen und Konflikte, damit Sie eine benutzerdefinierte Installation des Produkts erstellen können. Während der Installation prüft Symantec Packager automatisch den Ordner "Packager/Products" auf Produktmoduldateien und importiert sie automatisch.

Symantec pcAnywhere enthält auf der Installations-CD eine Produktmoduldatei (Symantec pcAnywhere <Version>.PMI). Wenn Sie Symantec Packager von der pcAnywhere Installations-CD installieren, importiert Symantec Packager diese Produktmoduldatei automatisch.

Wenn Sie Symantec Packager öffnen und auf der Registerkarte "Produkte importieren" keine Produkte angezeigt werden, müssen Sie das Produktmodul manuell importieren.

So importieren Sie ein Produktmodul:

1. Öffnen Sie Symantec Packager.
2. Klicken Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte importieren" im Menü "Datei" auf "Neues Produkt importieren".
3. Navigieren Sie im Dialogfeld "Öffnen" zu dem Ordner, in dem das zu importierende Produktmodul abgelegt ist.
4. Wählen Sie das Produktmodul aus, und klicken Sie anschließend auf "Öffnen".

   Symantec Packager importiert das Produktmodul und kehrt anschließend zur Registerkarte "Produkte importieren" zurück. Abhängig von der Größe und Komplexität des Produktmoduls kann der Registrierungsprozess einige Zeit in Anspruch nehmen.

Anpassen der Produkteinstellungen

Symantec Packager erstellt für jedes Produktmodul, das Sie in Symantec Packager importieren, eine standardmäßige Produktkonfigurationsdatei (.pcg). Jede Produktkonfigurationsdatei enthält die Funktionen, Installationsoptionen und vorkonfigurierten Einstellungen, die im Produkt enthalten sein sollen. Symantec Packager verwendet diese Informationen, um Installationspakete zusammenzustellen.

Sie können die standardmäßige Produktkonfigurationsdatei bearbeiten oder eine neue Datei erstellen. In Tabelle 2-1 finden Sie eine Übersicht über die Konfigurationsoptionen, die in der standardmäßige Produktkonfigurationsdatei von pcAnywhere verfügbar sind.

Tabelle 2-1 Symantec pcAnywhere-Produktkonfigurationsoptionen

Registerkarte	Einstellungen
Funktionen	In pcAnywhere können Sie die folgenden Funktionen anpassen: ■ Benutzeroberfläche (pcAnywhere-Manager) ■ Remote-Komponenten ■ Host-Komponenten ■ Kommunikationsprotokolle ■ OLE-Automatisierung ■ Ereignisprotokollierung ■ pcAnywhere Administrator-Tools (Host-Administrator und Remote Access Perimeter Scanner) ■ Dokumentation (Online-Handbücher und Hilfe) ■ Symantec-Installationsprogramme ■ Microsoft-Systemkomponenten
Konfigurationsdateien	Die pcAnywhere-Produktvorlage enthält standardmäßige Remote- und Host-Konfigurationsobjekte, die Sie nach der Installation des Pakets oder des benutzerdefinierten Produkts konfigurieren können. Zur weiteren Anpassung können Sie in pcAnywhere erstellte Konfigurationsdateien zum Paket oder zur angepassten Produktinstallation hinzufügen.

Tabelle 2-1 Symantec pcAnywhere-Produktkonfigurationsoptionen

Registerkarte	Einstellungen
Installationsoptionen	Folgende Produktinstallationsoptionen können für pcAnywhere angepasst werden: ■ Produktbeschreibung ■ Zielablageort ■ Online-Registrierung beim Start ausführen ■ Als Vorlage zu verwendendes Host-Objekt ■ Mit Windows zu startendes Host-Objekt ■ Als Vorlage zu verwendendes Remote-Objekt ■ LiveUpdate nach dem Start ausführen ■ Vorhandene Konfigurationseinstellungen beibehalten

Wenn Sie die Produktfunktionen, die Installationsoptionen und optionalen Dateien ausgewählt haben, die Sie in das benutzerdefinierte Produkt einbinden möchten, können Sie das Produkt zum Testen generieren. Beim Generieren der Produktkonfigurationsdatei wird eine Microsoft Installer-Datei (.msi) erstellt. Symantec Packager unterstützt nur die Installation von pcAnywhere .msi-Dateien.

Siehe "Produktkonfigurationsdatei generieren" auf Seite 46.

Produktfunktionen auswählen

In Symantec Packager können Sie Produktinstallationen anpassen, indem Sie die Funktionen einfügen, die Sie benötigen, und die Funktionen löschen, die Sie nicht benötigen. Die Größe des Produkts und der Installation sind von den von Ihnen gewählten Funktionen abhängig.

Manche Funktionen in pcAnywhere hängen von anderen Komponenten ab. Obwohl Symantec Packager automatisch nach Abhängigkeiten sucht, ist es möglich, dass Sie ein pcAnywhere-Installationspaket erstellen, das nicht alle erforderlichen Dateien enthält.

Lesen Sie beim Auswählen von Produktfunktionen, die in ein Paket ein- oder ausgeschlossen werden sollen, die Funktionsbeschreibungen. Diese werden im Fenster "Produkteditor" auf der Registerkarte "Funktionen" angezeigt. Die Funktionsbeschreibungen informieren über Abhängigkeiten, die zwischen Funktionen bestehen können. In Tabelle 2-2 finden Sie eine Übersicht über die Produktabhängigkeiten. Diese Liste ist nicht vollständig.

Tabelle 2-2 Symantec pcAnywhere-Produktabhängigkeiten

Funktion	Abhängigkeit
pcAnywhere-Manager	Erforderlich, wenn Benutzer in der Lage sein sollen, Konfigurationseinstellungen zu ändern. Schließen Sie pcAnywhere-Manager aus, wenn Sie die Integrationsverwaltung einschließen möchten.
Remote	Erfordert mindestens ein Kommunikationsprotokoll.
Host	Erfordert eine Anruferkonfigurationsdatei (.cif), wenn für das Produkt beim Starten automatisch ein Host gestartet werden soll. Erfordert mindestens einen Authentifizierungstyp. Erfordert mindestens ein Kommunikationsprotokoll.
Fernsteuerung	Für alle angepassten Produktinstallationen erforderlich.
Dateiübertragung	Erfordert mindestens ein Kommunikationsprotokoll.
Fernverwaltung	Erfordert mindestens ein Kommunikationsprotokoll.
Dialog	Erfordert mindestens ein Kommunikationsprotokoll.
Authentifizierung	Für alle angepassten Produktinstallationen erforderlich.
Kommunikationsprotokolle	Für alle angepassten Produktinstallationen erforderlich.

So wählen Sie Produktfunktionen aus:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Führen Sie im Dialogfeld "Produkteditor" auf der Registerkarte "Funktionen" einen der folgenden Schritte aus:
   - Aktivieren Sie die Produktfunktionen, die im benutzerdefinierten Produkt enthalten sein sollen.
   - Deaktivieren Sie die Funktionen, die nicht erforderlich sind.
   - Klicken Sie auf das Pluszeichen neben einer Funktion, um die Teilfunktionen auszuwählen oder sie zu entfernen.
3. Wählen Sie eine der folgenden Optionen aus:
   - OK: Speichert die von Ihnen durchgeführten Änderungen und schließt das Dialogfeld "Produkteditor".
   - Übernehmen: Speichert die von Ihnen durchgeführten Änderungen und lässt Sie mit der Produktkonfiguration fortfahren.
4. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Konfigurationsdateien einbinden

In Symantec Packager können Sie vorkonfigurierte Daten- oder Konfigurationsdateien verwenden, so dass die Benutzer während oder nach der Installation keine Konfigurationsänderungen mehr vornehmen müssen. Für produktspezifische Konfigurationen müssen Sie diese Dateien zunächst im Produkt konfigurieren und danach zur Registerkarte "Konfigurationsdateien" in Symantec Packager hinzufügen. Konfigurationsdateien können nicht in Symantec Packager bearbeitet werden.

Weitere Informationen dazu finden Sie in der Online-Hilfe zu Symantec Packager.

Die pcAnywhere-Produktvorlage enthält in Abhängigkeit von den Funktionen, die Sie auf der Registerkarte "Funktionen" ausgewählt haben, die folgenden Standardkonfigurationsdateien:

Symantec LiveUpdate-Datei (LIVEUPDT.HIST)	Enthält die Informationen, die für Verbindungen zum Symantec LiveUpdate-Server erforderlich sind, um automatische Produktaktualisierungen für Ihre Version von pcAnywhere zu erhalten.
Remote-Verbindungsobjektdateien (.chf)	Enthalten Standardeinstellungen für die Unterstützung von Verbindungen zu einem Host-Computer über eine Modem-, Netzwerk- oder Direktverbindung. Darüber hinaus sind Standardeinstellungen zum Herstellen einer Verbindung im Dateiübertragungs- oder Fernverwaltungsmodus vorhanden.
Host-Verbindungsobjektdateien (.bhf)	Enthalten Standardeinstellungen, damit Remote-Benutzer Verbindungen zu einem Computer über eine Modem-, Netzwerk- oder Direktverbindung herstellen können.

Abhängig von den Funktionen, die Sie auf der Registerkarte "Funktionen" ausgewählt haben, können Sie die folgenden Dateien in pcAnywhere konfigurieren und zur angepassten Produktinstallation hinzufügen:

Optionsgruppe	Hiermit konfigurieren Sie globale Optionen für pcAnywhere, um spezielle Konfigurationsanforderungen zu berücksichtigen.
Host-Sicherheits-IDs	Hiermit versehen Sie die pcAnywhere-Installation mit einer Seriennummer.
Remote-Verbindungsobjektdateien (.chf)	Hiermit können Sie vorab die Verbindungs- und Sicherheitseinstellungen konfigurieren, die zum Herstellen einer Fernverbindung zu einem anderen Computer erforderlich sind. Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Befehlswarteschlangendateien	Hiermit automatisieren Sie Dateiübertragungs-, Befehlszeilen- und Sitzungsendeaufgaben. Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
Host-Verbindungsobjektdateien (.bhf)	Hiermit können Sie vorab die Verbindungs- und Sicherheitseinstellungen konfigurieren, die für eine Verbindung von einem anderen Computer erforderlich sind. Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
Anruferdateien (.cif)	Hiermit können Sie vorab ein Anmeldekonto für Benutzer konfigurieren, die eine Verbindung zum Host-Computer herstellen, sowie eine Authentifizierungsmethode zum Überprüfen ihrer Identität auswählen. Diese Informationen sind zum Starten eines Hosts erforderlich. Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Symantec pcAnywhere-Konfigurationsdateien sind in den folgenden Ordnern gespeichert:

Windows 2000/XP	\Dokumente und Einstellungen\All Users\Anwendungsdaten\Symantec\pcAnywhere
Windows NT 4.0	\Winnt\Profiles\All Users\Anwendungsdaten\Symantec\pcAnywhere
Windows 98/Me	\Windows\All Users\Anwendungsdaten\Symantec\pcAnywhere

Diese Ordner werden standardmäßig vom Betriebssystem verborgen.
Um nach den pcAnywhere-Konfigurationsdateien zu suchen, müssen Sie die Ordneroptionen Ihres Betriebssystems bearbeiten und die Option für die Anzeige von versteckten Dateien aktivieren.

Darüber hinaus können Sie Registrierungsschlüsseldateien hinzufügen, um bestimmte pcAnywhere-Einstellungen zu steuern. Die Registrierungsschlüssel in der Datei werden zur Systemregistrierung auf dem Zielcomputer hinzugefügt, wenn das Paket oder das angepasste Produkt installiert wird.

Warnung: Konfigurieren Sie eine Registrierungsschlüsseldatei nur mit äußerster Vorsicht. Eine falsche Einstellung kann dazu führen, dass das Betriebssystem bzw. das Produkt nicht mehr funktionsfähig ist.

So fügen Sie eine Konfigurationsdatei hinzu:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Führen Sie im Dialogfeld "Produkteditor" auf der Registerkarte "Konfigurationsdateien" einen der folgenden Schritte aus:
   - Wählen Sie den Typ der vorkonfigurierten Datei aus, die Sie hinzufügen möchten, und klicken Sie dann auf "Hinzufügen".

     Suchen Sie die Konfigurationsdatei, die Sie einschließen möchten, und klicken Sie dann auf "Öffnen". Die Symantec pcAnywhere-Konfigurationsdateien werden zur Liste hinzugefügt. Bei anderen Konfigurationsdateitypen wird die Standarddatendatei durch die vorkonfigurierte Datei ersetzt.
   - Wählen Sie die zu entfernende Datei aus, und klicken Sie anschließend auf "Entfernen".

     Dadurch wird die vorkonfigurierte Datei entfernt und, soweit vorhanden, durch die von Symantec zur Verfügung gestellte Standarddatendatei ersetzt.
3. Führen Sie im Dialogfeld "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
4. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Integritätsprüfung einer Produktkonfiguration

Verhindern Sie unzulässige Änderungen an einem installierten Produkt, indem Sie im Produkteditor auf der Registerkarte "Funktionen" die Funktion "Integritätsverwaltung" auswählen. Wenn pcAnywhere feststellt, dass eine Programm-, Registrierungs- oder Konfigurationsdatei in dem installierten, integritätsgeprüften pcAnywhere-Paket geändert wurde, wird pcAnywhere nicht ausgeführt.

Wenn Sie die Integritätsverwaltungsfunktion auswählen, müssen Sie pcAnywhere-Manager und LiveUpdate ausschließen. Nach der Installation eines integritätsgeprüften Pakets können Benutzer pcAnywhere weder ändern noch aktualisieren. Auch die Installation von Software-Upgrades mit Hilfe von LiveUpdate ist dann nicht möglich. Sie müssen ein neues Paket erstellen und installieren, wenn Aktualisierungen erforderlich sind.

Bei einer Verletzung der Integrität, einschließlich Änderungen an der Registrierung sowie Hinzufügen oder Löschen von Dateien, wird das Programm möglicherweise nicht mehr ausgeführt. Setzen Sie die Integritätsprüfung zusammen mit der Richtlinienverwaltung und umfassenden Sicherheitsmaßnahmen (z.B. Betriebssystem-Hardening) ein.

Siehe "Konfigurieren einer richtliniengestützten Verwaltung" auf Seite 149.

So führen Sie eine Integritätsprüfung einer Produktkonfiguration durch:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Klicken Sie im Fenster "Produkteditor" auf der Registerkarte "Funktionen" auf das Pluszeichen neben den Symantec-Installationsprogrammen, um die Liste zu erweitern.
3. Aktivieren Sie "Integritätsverwaltung".
4. Wählen Sie weitere Funktionen aus, die für das Produkt ein- oder ausgeschlossen werden sollen.
5. Wählen Sie auf der Registerkarte "Installationsoptionen" die gewünschten Produktinstallationsoptionen aus.
   Siehe "Produktinstallationsoptionen festlegen" auf Seite 36.

6. Wählen Sie eine der folgenden Optionen aus:
   - OK: Speichert die von Ihnen durchgeführten Änderungen und schließt das Dialogfeld "Produkteditor".
   - Übernehmen: Speichert die von Ihnen durchgeführten Änderungen und lässt Sie mit der Produktkonfiguration fortfahren.
7. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".
8. Generieren Sie eine Produktinstallation oder ein Paket.

   Beim Generieren einer Produktkonfigurationsdatei wird eine .msi-Datei erstellt, die das Produkt enthält.

   Sie können die Produktkonfigurationsdatei zu einem Paket hinzufügen, um die Installation weiter anzupassen. Beim Generieren eines Pakets wird eine selbstextrahierende .exe-Datei erstellt.

pcAnywhere-Installation eine Seriennummer zuweisen

Mit Symantec pcAnywhere können Sie ein angepasstes Installationspaket mit einem Sicherheitscode versehen, indem Sie eine Seriennummer integrieren. Diese Seriennummer muss auf dem Host- und dem Remote-Computer vorhanden sein, um eine Verbindung herzustellen.

Die Zuweisung einer Seriennummer umfasst folgende Schritte:

- Generieren Sie in pcAnywhere eine Seriennummerndatei (.SID).
- Wählen Sie in Symantec Packager im Produkteditor die gewünschten Funktionskomponenten aus, und fügen Sie dann die Seriennummer-Konfigurationsdatei hinzu.
- Generieren Sie das Paket.
- Verteilen und installieren Sie das Paket.

Seriennummerndatei generieren

In Symantec pcAnywhere können Sie einen Sicherheitscode in Form einer Seriennummer generieren, die in eine angepasste Installation integriert werden kann. Die Seriennummer muss numerisch sein und darf nicht mehr als 10 Ziffern umfassen. Damit ein Remote-Benutzer eine Verbindung zu einem Host-Computer herstellen kann, auf dem eine andere Seriennummer verwendet wird, müssen Sie die Seriennummern für jeden Host-Computer in die Seriennummerndatei einfügen.

So generieren Sie eine Seriennummerndatei:

1. Klicken Sie in pcAnywhere-Manager in der linken Navigationsleiste auf "Seriennummern".
2. Klicken Sie im Menü "Datei" auf "Neu > Objekt > Weitere Optionen".
3. Geben Sie im Fenster "Eigenschaften für Seriennummern" unter "Host-Verbindungen mit Hilfe der folgenden Seriennummern begrenzen" die gewünschte Seriennummer ein.
4. Klicken Sie auf "Hinzuf ügen".
5. Klicken Sie auf "OK".
   Die Seriennummerndatei wird im rechten Fenster unter "Seriennummern" hinzugefügt.

Installationsdatei mit einer Seriennummer erstellen

Um eine pcAnywhere-Version mit einer Seriennummer zu erstellen, müssen Sie die in pcAnywhere generierte Seriennummerndatei zu einer Produktdefinitionsdatei hinzufügen. Die Seriennummer wird beim Zusammenstellen des Produkts oder eines Pakets, das die Produktdefinition enthält, in das Produkt integriert.

Die benutzerdefinierten Produktinstallationen bzw. Pakete müssen auf den Host- und Remote-Computern installiert werden. Damit zwischen einem Host- und Remote-Computer eine Verbindung hergestellt werden kann, müssen auf beiden Rechnern identische Seriennummern vorhanden sein.

So erstellen Sie eine Installationsdatei mit einer Seriennummer:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Führen Sie im Dialogfeld "Produkteditor" auf der Registerkarte "Funktionen" einen der folgenden Schritte aus:
   - Aktivieren Sie die Produktfunktionen, die im benutzerdefinierten Produkt enthalten sein sollen.
   - Deaktivieren Sie die Funktionen, die nicht erforderlich sind.
   - Klicken Sie auf das Pluszeichen neben einer Funktion, um die Teilfunktionen auszuwählen oder sie zu entfernen.

   Wählen Sie "Host und Remote" aus, um eine angepasste Produktinstallation oder ein angepasstes Paket zu konfigurieren, die bzw. das Host- und Remote-Funktionen enthält. Wählen Sie nur "Host" oder "Remote" aus, um separate Installationen zu erstellen.
3. Klicken Sie auf der Registerkarte "Konfigurationsdateien" auf "Seriennummerndateien (*.sid)" und dann auf "Hinzufügen".
4. Wechseln Sie in den Ordner, in dem die Seriennummerndatei (*.sid) gespeichert sind, die Sie in pcAnywhere generiert haben. Markieren Sie die gewünschte Datei, und klicken Sie auf "Öffnen".

   Die Seriennummerndatei wird zur Liste der Daten und Konfigurationsdateien hinzugefügt.
5. Wählen Sie auf der Registerkarte "Installationsoptionen" die gewünschten Produktinstallationsoptionen aus.

   Siehe "Produktinstallationsoptionen festlegen" auf Seite 36.
6. Wählen Sie eine der folgenden Optionen aus:
   - OK: Speichert die von Ihnen durchgeführten Änderungen und schließt das Dialogfeld "Produkteditor".
   - Übernehmen: Speichert die von Ihnen durchgeführten Änderungen und lässt Sie mit der Produktkonfiguration fortfahren.
7. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

8 Generieren Sie eine Produktinstallation oder ein Paket.

Beim Generieren einer Produktkonfigurationsdatei wird eine .msi-Datei erstellt, die ein Einzelprodukt enthält.

Sie können die Produktkonfigurationsdatei zu einem Paket hinzufügen, um die Installation weiter anzupassen. Beim Generieren eines Pakets wird eine selbstextrahierende .exe-Datei erstellt.

Konfigurationseinstellungen global verwalten

Mit Symantec pcAnywhere-Optionsgruppen können Sie die globalen Einstellungen für Host- und Remote-Verbindungen sowie für die Dateiübertragung, die Protokollierung und weitere Funktionen verwalten, um die Leistung und die Sicherheit zu optimieren oder Verbindungen zu verwalten. In Symantec pcAnywhere können mehrere Optionsgruppen erstellt werden, um spezielle Konfigurationsanforderungen zu berücksichtigen.

Vorkonfigurierte Optionsgruppen können für benutzerdefinierte Installationspakete verwendet werden, die mit Symantec Packager erstellt wurden. Sie können auch als Standardeinstellungen für den lokalen Computer dienen.

Optionsgruppe in pcAnywhere konfigurieren

Symantec pcAnywhere gruppiert die Optionsgruppeneigenschaften auf Registerkarten. In Tabelle 2-3 finden Sie Informationen, wo Sie die entsprechenden Einstellungen finden.

Tabelle 2-3 Eigenschaften für Symantec pcAnywhere-Optionsgruppen

Registerkarte	Beschreibung
Host-Operation	Hiermit können einfache Host-Operationen konfiguriert werden, z. B. Host-Name und Datensatzeinstellungen.
Remote-Operation	Hiermit werden die Leistungs- und Anzeigeeinstellungen für Remote-Sitzungen konfiguriert.
Host-Kommunikation	Enthält Anpassungsoptionen für Modem- und Netzwerkverbindungen auf dem Host.
Remote-Kommunikation	Enthält Anpassungsoptionen für Modem- und Netzwerkverbindungen auf dem Remote.
Sitzungs-Manager	Steuert grundlegende Sitzungsoptionen, wie z. B. die Hintergrundfarbe für den nicht verwendbaren Bereich des Remote-Desktops, und ermöglicht das Anzeigen oder Bearbeiten der Eingabeaufforderungs-Ausnahmeliste.

Tabelle 2-3 Eigenschaften für Symantec pcAnywhere-Optionsgruppen

Registerkarte	Beschreibung
Dateiübertragung	Hiermit werden Dateiübertragungseinstellungen konfiguriert.
Ereignisprotokollierung	Aktiviert die Protokollierung von Ereignissen, die während einer pcAnywhere-Sitzung stattfinden.
Verzeichnisdienste	Hiermit werden Einstellungen konfiguriert, die die Verwendung eines Verzeichnisdiensts zum Auffinden von Hosts steuern.
Remote-Drucken	Enthält Einstellungen für das Konfigurieren der Remote-Druckfunktion.
Datenverschlüsselung	Hiermit werden für das Verschlüsseln mit dem öffentlichen Schlüssel benötigte Zertifikatsinformationen angegeben.

So konfigurieren Sie eine Optionsgruppe in pcAnywhere:

1. Klicken Sie in pcAnywhere-Manager in der linken Navigationsleiste auf "Optionsgruppen".
2. Führen Sie eine der folgenden Aktionen aus:
   - Um eine neue Optionsgruppe zu erstellen, klicken Sie im Menü "Datei" auf "Neu" > Objekt > Weitere Optionen".
   - Um eine vorhandene Optionsgruppe zu ändern, klicken Sie im rechten Fenster mit der rechten Maustaste auf die Optionsgruppe, und klicken Sie dann auf "Eigenschaften".
3. Führen Sie im Eigenschaftenfenster für die Optionsgruppe mit Hilfe des Pfeils nach links bzw. rechts einen Bildlauf in der Registerkartenliste durch.

   Siehe Tabelle 2-3, "Eigenschaften für Symantec pcAnywhere-Optionsgruppen," auf Seite 33.
4. Konfigurieren Sie die Einstellungen, die Sie verwenden möchten.
5. Wenn Sie alle gewünschten Einstellungen geändert haben, klicken Sie auf "OK".

   Weitere Informationen zu Funktionen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Optionsgruppe zu einer angepassten Installationsdatei hinzufügen

Die Optionsgruppen, die Sie in pcAnywhere erstellen, können Sie zu einer angepassten Installationsdatei hinzufügen. Nachdem das Paket oder das angepasste Produkt auf dem Zielcomputer installiert wurde, kann die Optionsgruppe auf dem lokalen Computer verwendet werden.

So fügen Sie eine Optionsgruppe zu einer angepassten Installationsdatei hinzu:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Klicken Sie im Fenster "Produkteditor" auf der Registerkarte "Konfigurationsdateien" auf "Optionsgruppendatei (*.OPT)" und dann auf "Hinzufügen".
3. Wechseln Sie in den Ordner, in dem die Optionsgruppendateien (*.opt) gespeichert sind, die Sie in pcAnywhere erstellt haben. Markieren Sie die gewünschte Datei, und klicken Sie auf "Öffnen".

   Die Optionsgruppendatei wird zur Liste der Daten- und Konfigurationsdateien hinzugefügt.
4. Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
5. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Optionsgruppe auf den lokalen Computer übernehmen

In Symantec pcAnywhere können mehrere Optionsgruppendateien verwaltet werden, um spezielle Konfigurationsanforderungen zu berücksichtigen. Beispiel: Wenn Sie an unterschiedlichen Standorten arbeiten, können Sie vermeiden, die Standardeinstellungen bei jedem Standortwechsel ändern zu müssen. Erstellen Sie dazu für jeden Standort eine Optionsgruppe, und übernehmen Sie sie bei Ihrer Ankunft an dem betreffenden Standort. Wenn Sie eine Optionsgruppe auf den lokalen Computer übernehmen, werden die Standardeinstellungen in pcAnywhere überschrieben.

So übernehmen Sie eine Optionsgruppe auf den lokalen Computer:

1. Klicken Sie in pcAnywhere-Manager in der linken Navigationsleiste auf "Optionsgruppen".
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die gewünschte Optionsgruppe, und klicken Sie anschließend auf "In lokales System übernehmen".

Produktinstallationsoptionen festlegen

In Symantec Packager können Sie Installationsoptionen für das Produkt festlegen, die vom jeweiligen Produkt und den Funktionen, die Sie zur Produktkonfiguration hinzugefügt haben, abhängen.

Es gibt weitere Installationsoptionen, die Sie auf Paketebene festlegen können. Dazu gehören Optionen für den Installationsmodus, den Neustart, die Protokollierung und die Wiederherstellung.

Weitere Informationen dazu finden Sie in der Online-Hilfe zu Symantec Packager.

In Symantec pcAnywhere können Sie die folgenden Installationsoptionen anpassen:

Beschreibung	Hiermit können Sie eine eindeutige Beschreibung für das Produkt angeben.
Zielablageort	Hiermit wählen Sie das Verzeichnis aus, in dem das Produkt auf dem Zielcomputer installiert werden soll. Siehe "Zielinstallationsverzeichnis ändern" auf Seite 37.
Online-Registrierung beim Programmstart starten	Hiermit werden Benutzer zur Registrierung des Produkts aufgefordert, wenn sie das Programm zum ersten Mal starten. Siehe "Benutzer beim Starten zum Registrieren auffordern" auf Seite 38.
Als Vorlage zu verwendendes Host-Objekt	Hiermit wählen Sie die Host-Konfigurationsdatei aus, die für neue Host-Verbindungsobjekte, die der Benutzer nach der Installation erstellt, als Vorlage verwendet werden soll. Siehe "Standardvorlage für Host-Verbindungen auswählen" auf Seite 39.

Mit Windows zu startendes Host-Objekt	Hiermit wählen Sie ein Host-Verbindungsobjekt aus, das automatisch gestartet wird, wenn der Benutzer auf dem Zielcomputer Windows startet. Siehe "Standardvorlage für Host-Verbindungen auswählen" auf Seite 39.
Als Vorlage zu verwendendes Remote-Objekt	Hiermit wählen Sie die Remote-Konfigurationsdatei aus, die für neue Remote-Verbindungsobjekte, die der Benutzer nach der Installation erstellt, als Vorlage verwendet werden soll. Siehe "Standardvorlage für Remote-Verbindungen auswählen" auf Seite 40.
LiveUpdate nach der Installation ausführen	Hiermit wird die benutzerdefinierte Installation so konfiguriert, dass automatisch eine Verbindung zum Symantec LiveUpdate-Server hergestellt wird, um Produktaktualisierungen herunterzuladen. Siehe "Produkte aktualisieren" auf Seite 41.
Vorhandene Konfigurations-einstellungen beibehalten	Hiermit wird das Produkt so konfiguriert, dass vorhandene Konfigurationseinstellungen beibehalten werden, wenn Sie über eine vorherige Version von pcAnywhere installieren.

Zielinstallationsverzeichnis ändern

Angepasste Symantec pcAnywhere-Installationen, die Sie mit Symantec Packager erstellen, werden standardmäßig im Verzeichnis "Programme" unter "Symantec\pcAnywhere" installiert. Sie können hier auch ein anderes Verzeichnis angeben.

So ändern Sie das Zielinstallationsverzeichnis:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "Zielablageort".

3 Wählen Sie im Fenster "Zielablageort" eine der folgenden Optionen aus:

- Verzeichnis der Programmdateien
- Stammverzeichnis des Systemlaufwerks
- Benutzerdefinierter Pfad
  Geben Sie unter "Ordner" den vollständige Pfad zum Speicherort ein, in dem das Produkt installiert werden soll.

4 Klicken Sie auf "OK".

5 Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:

- Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
- Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.

6 Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Benutzer beim Starten zum Registrieren auffordern

Mit Symantec Packager können Sie das Produkt so konfigurieren, dass Benutzer zur Online-Registrierung aufgefordert werden, wenn sie das Produkt zum ersten Mal starten. Um diese Installationsoption zu verwenden, müssen Sie die pcAnywhere-Manager-Funktion zur Produktkonfiguration hinzufügen.

So werden Benutzer beim Starten zum Registrieren aufgefordert:

1 Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:

- Erstellen Sie eine neue Produktkonfiguration.
- Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.

2 Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "Online-Registrierung beim Start ausführen".

3 Aktivieren Sie im Fenster "Online-Registrierung beim Start ausführen" das Kontrollkästchen "Online-Registrierung beim Start ausführen".

4 Klicken Sie auf "OK".

5 Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:

- Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
- Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.

6 Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Standardvorlage für Host-Verbindungen auswählen

Mit Symantec Packager können Sie die Host-Konfigurationsdatei auswählen, die für neue Host-Verbindungsobjekte, die der Benutzer nach der Installation erstellt, als Vorlage verwendet werden soll. Host-Verbindungsobjekte enthalten die Konfigurationseinstellungen, damit Remote-Benutzer eine Verbindung zum Host-Computer herstellen können.

Sie können die Standardeinstellungen von pcAnywhere, ein vorkonfiguriertes Host-Verbindungsobjekt von pcAnywhere oder ein Host-Verbindungsobjekt eines Benutzers auswählen.

So wählen Sie die Standardvorlage für Host-Verbindungen aus:

1 Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:

- Erstellen Sie eine neue Produktkonfiguration.
- Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.

2 Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "Als Vorlage zu verwendendes Host-Objekt".

3 Wählen Sie im Fenster "Als Vorlage zu verwendendes Host-Objekt" unter "Wert" die Host-Verbindungsobjektdatei (.bhf) aus, die Sie als Vorlage verwenden möchten.

4 Klicken Sie auf "OK".

5 Um das Produkt so zu konfigurieren, dass ein Host automatisch gestartet wird, wenn der Benutzer Windows startet, doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf Mit Windows zu startendes Host-Objekt".

6 Wählen Sie im Fenster "Mit Windows zu startendes Host-Objekt" unter "Wert" die gewünschte BHF-Datei aus.

7. Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
8. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Standardvorlage für Remote-Verbindungen auswählen

Mit Symantec Packager können Sie die Remote-Konfigurationsdatei auswählen, die für neue Remote-Verbindungsobjekte, die der Benutzer nach der Installation erstellt, als Vorlage verwendet werden soll. Remote-Verbindungsobjekte enthalten die Konfigurationseinstellungen zum Herstellen einer Remote-Verbindung zu einem anderen Computer.

Sie können die Standardeinstellungen von pcAnywhere, ein vorkonfiguriertes Remote-Verbindungsobjekt von pcAnywhere oder ein Remote-Verbindungsobjekt eines Benutzers auswählen.

So wählen Sie die Standardvorlage für Remote-Verbindungen aus:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "Als Vorlage zu verwendendes Remote-Objekt".
3. Wählen Sie im Fenster "Als Vorlage zu verwendendes Remote-Objekt" unter "Wert" die Remote-Verbindungsobjektdatei (.chf) aus, die Sie als Vorlage verwenden möchten.
4. Klicken Sie auf "OK".
5. Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
6. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Produkte aktualisieren

Wenn Sie die LiveUpdate-Funktion in die Produktkonfiguration einbeziehen, können Sie mit Symantec Packager das Produkt so konfigurieren, dass nach der Installation automatisch eine Verbindung zum Symantec LiveUpdate-Server hergestellt wird, um Produktaktualisierungen herunterzuladen.

Wenn Sie den Symantec LiveUpdate Administrator installiert haben, um darüber alle LiveUpdate-Vorgänge für ihr Netzwerk abzuwickeln, dann können Sie das Produkt so konfigurieren, dass eine Verbindung zum LiveUpdate-Server in Ihrem Netzwerk hergestellt wird. Sie müssen die LiveUpdate-Konfigurationsdatei (LIVEUPDT.HST) anpassen und den Pfad zum LiveUpdate-Server hinzufügen.

Weitere Informationen finden Sie in der LiveUpdate-Dokumentation.

So aktualisieren Sie Produkte:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "LiveUpdate nach dem Start ausführen".
3. Aktivieren Sie im Fenster "LiveUpdate nach dem Start ausführen" das Kontrollkästchen "LiveUpdate nach dem Start ausführen".
4. Klicken Sie auf "OK".
5. Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
6. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Bestehende Konfigurationseinstellungen beibehalten

Wenn Sie ein Paket über eine bestehende Version von pcAnywhere installieren (ab Version 10.0), können Sie mit Symantec Packager die Registrierungs-, Host-, Remote- und Anrufer-Konfigurationseinstellungen beibehalten.

Siehe "Wenn eine vorherige Version installiert ist" auf Seite 11.

Diese Option ist nur für Installationen ohne Ausgabe sowie passive Installationen verfügbar. Installationsmoduseinstellungen müssen Sie auf der Paketebene konfigurieren.

Siehe "Erstellen von Installationspaketen" auf Seite 44.

So behalten Sie bestehende Konfigurationseinstellungen bei:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Produktkonfiguration.
   - Doppelklicken Sie auf ein Produkt, um es zu bearbeiten.
2. Doppelklicken Sie im Fenster "Produkteditor" auf der Registerkarte "Installationsoptionen" auf "Vorhandene Konfigurationseinstellungen beibehalten".
3. Aktivieren Sie im Fenster "Vorhandene Konfigurationseinstellungen beibehalten" das Kontrollkästchen "Vorhandene Konfigurationseinstellungen beibehalten".
4. Klicken Sie auf "OK".
5. Führen Sie im Fenster "Produkteditor" einen der folgenden Schritte aus:
   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Produkteditor" zu schließen.
   - Klicken Sie auf "Übernehmen", um die Änderungen zu speichern und mit der Produktkonfiguration fortzufahren.
6. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Erstellen eines benutzerdefinierten Befehls

Zusätzlich zum Erstellen benutzerdefinierter Produkte können Sie auch benutzerdefinierte Befehle in Ihre Pakete aufnehmen. Beispiele für benutzerdefinierte Befehle sind Stapeldateien, ausführbare Programmdateien von Fremdherstellern, Befehlszeilenargumente oder einfache Dateikopien. Mit benutzerdefinierten Befehlen können Sie die Anwendungsnutzung vereinfachen, indem Sie einem Paket mehrere Aufgaben hinzufügen. Wenn benutzerdefinierte Befehle einmal definiert sind, können sie in unterschiedlichen Paketen wiederverwendet werden.

Wenn Sie einen benutzerdefinierten Befehl erstellen, generiert Symantec Packager eine Befehlskonfigurationsdatei. Eine Befehlskonfigurationsdatei ist eine generische Produktkonfigurationsdatei, die nicht auf eine Produktvorlagendatei verweist. Daher ist es für benutzerdefinierte Befehle nicht erforderlich, ein Produktmodul zu importieren. Der Generierungsprozess für benutzerdefinierte Befehle erstellt eine selbstextrahierende Datei (.exe), die vor dem Einfügen in ein Paket getestet werden kann.

Symantec pcAnywhere-Pakete erfordern keine benutzerdefinierten Befehle. Weitere Informationen zu benutzerdefinierten Befehlen finden Sie in der Online-Hilfe zu Symantec Packager.

So erstellen Sie einen benutzerdefinierten Befehl:

1. Klicken Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" im Menü "Datei" auf "Neuer benutzerdefinierter Befehl".
2. Doppelklicken Sie im Dialogfeld "Befehlseditor" auf der Registerkarte "Parameter" auf "Beschreibung".
3. Geben Sie im Fenster "Befehlsbeschreibung" einen aussagefähigen Namen für den Befehl ein, so dass Sie ihn später leicht erkennen können.

   Beispiel:

   Deinstallation von pcAnywhere 9.0 ohne Benutzereingriff
4. Klicken Sie auf "OK".
5. Doppelklicken Sie im Dialogfeld "Befehlseditor" auf der Registerkarte "Parameter" auf "Befehlszeile".

6. Geben Sie im Fenster "Befehlszeilenspezifikation" unter "Befehlszeile und Schalter" den Befehl und die Befehlszeilenargumente ein, die zur Ausführung des Befehls erforderlich sind.

   Wenn Sie beispielsweise ein Deinstallationsprogramm für pcAnywhere 9.0 ohne Benutzereingriff ausführen möchten, geben Sie den vollständigen Pfad für die remove.exe-Datei zusammen mit dem Schalter /s ein. Die Datei befindet sich im pcAnywhere 9.0-Programmverzeichnis.

   "C:\Programme\Symantec\pcAnywhere\remove.exe" /s

   Sie müssen ein doppeltes Anführungszeichen vor und hinter dem vollständigen Pfad einfügen, damit das Betriebssystem im Pfad vorhandene Leerzeichen und lange Dateinamen korrekt verarbeitet.

7. Geben Sie unter "Optionale Schalter" die Befehlszeilenschalter ein, mit denen der Installationsablauf gesteuert werden soll.

8. Wählen Sie unter "Ausführungsoptionen" aus, wie dem Benutzer die Installation angezeigt werden soll.

9. Klicken Sie auf "OK".

Weitere Informationen zur Konfiguration von benutzerdefinierten Befehlen finden Sie in der Online-Hilfe zu Symantec Packager.

Erstellen von Installationspaketen

Mit Symantec Packager können Sie eine oder mehrere Produktkonfigurationsdateien und benutzerdefinierte Befehle zu einer Paketdefinitionsdatei zusammenfassen. Die Paketdefinition enthält Konfigurationsinformationen und Installationsanweisungen, die erforderlich sind, damit Symantec Packager das Paket generieren kann.

Das Erstellen von Paketen ist für angepasste pcAnywhere-Installationen optional. Mit Symantec Packager können Sie die Produktkonfigurationsdatei von Symantec pcAnywhere generieren. Dabei wird eine .msi-Datei erstellt, die lokal installiert oder aber verteilt werden kann. Sie können die Symantec pcAnywhere .msi-Datei mit einem Verteilungs-Tool eines anderen Herstellers verteilen. Mit dem Symantec Packager Verteilungs-Tool können keine .msi-Dateien verteilt werden.

Durch das Erstellen einer Paketdefinition können Sie folgende Aktionen ausführen:

- Eines oder mehrere Produkte und benutzerdefinierte Befehle zu einem Installationspaket zusammenstellen.
- Die Ausführung der Installation im interaktiven, passiven oder "Ohne Ausgabe"-Modus konfigurieren.
- Benutzerdefinierte Grafiken zu den Installationsfenstern für interaktive Installationen hinzufügen.
- Optionen für den Neustart konfigurieren, einschließlich der Aufforderung der Benutzer zum Speichern der Arbeit.
- Wiederherstellungsoptionen für eine fehlgeschlagene Installation auswählen.
- Eine Protokolldatei erstellen, um festzustellen, ob das Paket erfolgreich installiert wurde.
- Kontaktinformationen für die technische Unterstützung hinzufügen.

Weitere Informationen zum Konfigurieren von Paketeinstellungen finden Sie in der Online-Hilfe zu Symantec Packager.

Produkte und Befehle zu einer Paketdefinition hinzufügen

In Symantec Packager können Sie ein benutzerdefiniertes Installationspaket erstellen, das ein oder mehrere Produkte oder benutzerdefinierte Befehle enthält. Wenn Sie einer Paketdefinition ein Element hinzufügen oder es entfernen, werden seine in der Produktkonfigurationsdatei definierten Eigenschaften, sowie alle Produktanforderungen und eventuelle Konflikte im Dialogfeld "Paketeditor" angezeigt.

So fügen Sie Produkte und Befehle zu einer Paketdefinition hinzu:

1. Führen Sie im Fenster "Symantec Packager" auf der Registerkarte "Pakete konfigurieren" einen der folgenden Schritte aus:
   - Erstellen Sie eine neue Paketdefinition.
   - Doppelklicken Sie auf eine Paketdefinition, um sie zu bearbeiten.
2. Klicken Sie im Dialogfeld "Paketeditor" auf der Registerkarte "Produktauswahl" auf "Hinzufügen".
3. Wählen Sie im Fenster "Öffnen" das Produkt oder die benutzerdefinierte Befehlsdatei (.pcg), die Sie hinzufügen möchten.

4. Klicken Sie auf "Öffnen".

   Die voraussichtliche Größe des Pakets ändert sich abhängig von den enthaltenen Produkten oder Befehlen.

5. Wiederholen Sie die Schritte 2 bis 4, um weitere Produkte oder benutzerdefinierte Befehle hinzuzufügen.

6. Führen Sie im Fenster "Paketeditor" einen der folgenden Schritte aus:

   - Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld "Paketeditor" zu schließen.
   - Klicken Sie auf "OK", um die Änderungen zu speichern und mit der Konfiguration der Paketdefinition fortzufahren.

7. Geben Sie einen Dateinamen ein, und klicken Sie anschließend auf "Speichern".

Generieren von Produktinstallationen und Paketen

Wenn Sie den Inhalt und die Installationsoptionen für die Paketdefinitionsdatei definiert haben, müssen Sie die Paketdefinition generieren, um die Installationsdatei zu erstellen. Beim Generieren eines Pakets erstellt Symantec Packager eine selbstextrahierende ausführbare .exe-Datei, die die Produkt-, Befehls- und Paketoptionen enthält, die Sie festgelegt haben.

Mit Symantec Packager können Sie aber auch eine Produktkonfigurationsdatei erstellen. Dabei wird eine Microsoft Installer-Datei (.msi) für eine Einzelproduktinstallation erstellt.

Produktkonfigurationsdatei generieren

Beim Generieren einer Produktkonfigurationsdatei wird eine .msi-Datei erstellt, die Sie testen oder installieren können. Symantec Packager unterstützt die MSI-Installation nur für pcAnywhere-Produktmodule. Sie müssen keine Produktkonfigurationsdatei generieren, um sie zu einem Paket hinzuzufügen.

Symantec Packager speichert die .msi-Dateien im Symantec Packager-Datenverzeichnis. Sie können diese Dateien auf der Registerkarte "Pakete verteilen" anzeigen, wenn Sie die Einstellungen von Symantec Packager bearbeiten, um unterstützte .msi-Dateien anzuzeigen.

Sie können die pcAnywhere .msi-Datei mit entsprechenden Verteilungs-Tools anderer Hersteller verteilen. Mit dem Symantec Packager Verteilungs-Tool können keine .msi-Dateien verteilt werden.

So generieren Sie eine Produktkonfigurationsdatei:

1. Wählen Sie im Fenster "Symantec Packager" auf der Registerkarte "Produkte konfigurieren" die Produktkonfigurationsdatei aus, die Sie generieren möchten.
2. Klicken Sie im Menü "Datei" auf "Generieren".
   Im Fenster "Status der Produktgenerierung" werden Informationen über den Fortschritt des Generierungsprozesses angezeigt und alle Fehler protokolliert. Wenn die Generierung erfolgreich abgeschlossen wurde, lautet im Fenster "Status der Produktgenerierung" die letzte Zeile "Produkt wurde erfolgreich erstellt".
3. Klicken Sie im Fenster "Status der Produktgenerierung" auf "Schließen".

Paket generieren

Während des Generierungsprozesses ruft Symantec Packager Informationen aus den Paketdefinitions- und Produktkonfigurationsdateien ab, um zu ermitteln, welche Produkte, Produktfunktionen und benutzerdefinierten Einstellungen zur Installationsdatei hinzugefügt werden sollen. Anschließend prüft Symantec Packager den Inhalt des Pakets auf Produktkonflikte. Wenn Symantec Packager einen Produktkonflikt erkennt, wird der Generierungsprozess angehalten. Sie müssen diesen Konflikt beheben und anschließend den Generierungsprozess wiederholen.

Nach dem Prüfen auf Produktkonflikte überprüft Symantec Packager, ob die Produktanforderungen eingehalten wurden. In diesem Vorgang wird geprüft, ob alle erforderlichen Produkte der Paketdefinitionsdatei hinzugefügt wurden. Wenn Symantec Packager einen Fehler erkennt, erhält der Benutzer eine Fehlermeldung, wobei der Generierungsprozess jedoch fortgesetzt wird.

Wenn die Überprüfungsphasen abgeschlossen sind, erstellt Symantec Packager eine selbstextrahierende ausführbare Datei und fügt sie zum Testen und zum Verteilen an die lizenzierten Benutzer zur Registerkarte "Pakete verteilen" hinzu.

So generieren Sie ein Paket:

1. Wählen Sie im Fenster "Symantec Packager" auf der Registerkarte "Pakete konfigurieren" die Paketdefinitionsdatei aus, die Sie generieren möchten.
2. Klicken Sie im Menü "Datei" auf "Generieren".
   Im Fenster "Status der Paketgenerierung" werden Informationen über den Fortschritt des Generierungsprozesses angezeigt und alle Fehler protokolliert. Wenn die Paketgenerierung erfolgreich abgeschlossen wurde, lautet im Fenster "Status der Generierung" die letzte Zeile "Produkt wurde erfolgreich erstellt".
3. Klicken Sie im Dialogfeld "Status der Generierung" auf "Schließen".

Testen von Paketen

Es ist wichtig, dass Sie die Pakete vor dem Verteilen an die Endanwender testen, um die ordnungsgemäße Funktionalität sicherzustellen. Sie sollten die Paketverteilung und -installation in einer isolierten, kontrollierten Umgebung testen. Für den Test reichen ein oder zwei Testcomputer aus.

Obwohl während des Generierungsprozesses eine Fehlerprüfung stattfindet, können einige Fehler erst bei der Installation festgestellt werden. Dies trifft besonders dann zu, wenn das Paket ein Produkt enthält, für das ein Produkt eines Fremdherstellers erforderlich ist, oder wenn das Paket einen benutzerdefinierten Befehl enthält.

Während der Installation prüft Symantec Packager auf Produktkonflikte und stellt sicher, dass die erforderlichen Produkte auf dem Zielcomputer vorhanden sind. Wenn Symantec Packager einen Konflikt erkennt, den es nicht lösen kann, schlägt die Installation fehl. Testen Sie die Pakete, um sicherzustellen, dass die Produktanforderungen eingehalten wurden und die Installationsreihenfolge richtig ist.

Sie sollten zudem jedes installierte Programm starten, um sicherzustellen, dass es ordnungsgemäß funktioniert. Überprüfen Sie, ob alle gewünschten Funktionen vorhanden sind. Dieser Schritt ist besonders wichtig, wenn Sie ein Produkt so angepasst haben, dass der für die Installation benötigte Speicherplatz reduziert wird. Durch das Testen eines Produkts stellen Sie sicher, dass Sie keine wichtigen Funktionen übersehen haben. Sobald Sie das Paket sorgfältig geprüft haben, können Sie es an die Endanwender verteilen.

Kapitel 3

Verteilen angepasster Installationen von Symantec pcAnywhere

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zur Verteilung
- Informationen zu den Installationsdateiverzeichnissen
- Verteilen von Installationspaketen mit Hilfe der webbasierten Verteilung
- Verteilen von pcAnywhere mit Hilfe von SMS 2.0
- Windows NT/2000/XP-Anmeldeskripts
- NetWare-Anmeldeskripts

Informationen zur Verteilung

Die angepassten pcAnywhere-Installationen, die Sie mit Symantec Packager erstellen, und die vorkonfigurierten Installationen, die auf der Symantec pcAnywhere-CD enthalten sind, können Sie mit Hilfe folgender Methoden verteilen:

- Installation auf lokalem Computer

  Wenn Sie in Symantec Packager auf der Registerkarte "Pakete verteilen" eine ausführbare Datei (.exe) oder eine unterstützte .msi-Datei öffnen, wird der Installationsvorgang gestartet. Stellen Sie sicher, dass der Zielcomputer die Systemanforderungen für die pcAnywhere-Installation erfüllt.

  Weitere Informationen zur Verwendung der Registerkarte "Pakete verteilen" finden Sie im *Symantec Packager Implementierungshandbuch* auf der pcAnywhere-CD.

  Weitere Informationen zur Installation von pcAnywhere finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

- Symantec Packager Paketverteilungs-Tool

  Mit diesem Tool verteilen Sie Pakete an einen oder mehrere Computer im Netzwerk. Das Symantec Packager Paketverteilungs-Tool ermöglicht die Verteilung nur an Microsoft 32-Bit-Computer (z.B. Windows NT/2000/XP).

  Weitere Informationen finden Sie im *Symantec Packer Implementierungshandbuch* auf der pcAnywhere-CD.

- Webbasiertes Verteilungs-Tool von Symantec

  Mit diesem Tool verteilen Sie Paket- oder Produktinstallationen an einen oder mehrere Computer mit Hilfe eines Web-Servers.

  Siehe "Verteilen von Installationspaketen mit Hilfe der webbasierten Verteilung" auf Seite 51.

- Tools anderer Hersteller

  Mit Symantec Packager erstellte Paket- und Produktinstallationen können mit Hilfe eines Verteilungs-Tools eines Fremdherstellers wie z.B. Microsoft Systems Management Server (SMS) weitergegeben werden.

  Siehe "Verteilen von pcAnywhere mit Hilfe von SMS 2.0" auf Seite 61.

- Anmeldeskripts

  Mit Symantec Packager erstellte Paket- und Produktinstallationen können mit Hilfe eines Anmeldeskripts an Computer unter Windows NT/2000/XP und Novell NetWare verteilt werden.

  Siehe "Windows NT/2000/XP-Anmeldeskripts" auf Seite 65.

  Siehe "NetWare-Anmeldeskripts" auf Seite 67.

Informationen zu den Installationsdateiverzeichnissen

Vorkonfigurierte Paket- und Produktinstallationsdateien sind im Verzeichnis "Packages" auf der Symantec pcAnywhere-CD gespeichert. Paket- und Produktinstallationsdateien, die Sie mit Symantec Packager erstellen, werden in Symantec Packager auf der Registerkarte "Pakete verteilen" aufgeführt.

Zum Anzeigen von .msi-Dateien müssen Sie die Voreinstellungen von Symantec Packager bearbeiten, damit unterstützte .msi-Produktdateien aufgeführt werden. Symantec Packager unterstützt die MSI-Verteilung nur für pcAnywhere .msi-Dateien.

Weitere Informationen finden Sie in der Online-Hilfe zu Symantec Packager oder im *Symantec Packager Implementierungshandbuch* auf der pcAnywhere Installations-CD.

Verteilen von Installationspaketen mit Hilfe der webbasierten Verteilung

Pakete, die mit Symantec Packager erstellt werden, können mit Hilfe eines von Symantec bereitgestellten webbasierten Verteilungs-Tools in Ihrem unternehmenseigenen Intranet verteilt werden. Alle Quelldateien, die für die Implementierung einer webbasierten Verteilung benötigt werden, befinden sich auf der Symantec pcAnywhere-CD im Ordner "Tools/Web Deploy".

Für die Verteilung von Paketen mit Hilfe der webbasierten Verteilung sind die folgenden Schritte erforderlich:

- Lesen Sie die Anforderungen für die webbasierte Verteilung.
- Richten Sie den Installations-Web-Server ein. Dazu zählt das Kopieren der Paketdateien in das Verteilungsverzeichnis auf dem Web-Server.
- Bearbeiten Sie die Verteilungsdateien.
- Testen Sie die Installation.
- Informieren Sie die Benutzer über den Speicherort zum Herunterladen.

Das webbasierte Verteilungs-Tool unterstützt die Bereitstellung von Symantec Packager-Paketen und Microsoft Software Installer-Dateien (.msi). Mit Symantec Packager können Sie eine Paketinstallationsdatei als selbstextrahierende ausführbare Datei (.exe) oder aber eine angepasste Produktinstallation für ein einzelnes Produkt als .msi-Datei erstellen.

Anforderungen für die webbasierte Verteilung

Vor dem Implementieren der webbasierten Verteilung auf einem Web-Server oder Zielcomputer sollten Sie die in Tabelle 3-1 aufgeführten Anforderungen durchlesen.

Tabelle 3-1 Anforderungen an Web-Server und Zielcomputer

Verteilung auf	Anforderungen
Web-Server	■ HTTP-Web-Server ■ Microsoft Internet Information Server (IIS), Version 4.0/5.0 ■ Apache HTTP Server ab Version 1.3 UNIX- und Linux-Plattformen werden ebenfalls unterstützt.
Zielcomputer	■ Internet Explorer ab Version 4.0 Für die Installation von Symantec pcAnywhere ist Internet Explorer ab Version 5.5 SP2 erforderlich. ■ Windows Installer ab Version 2.0 (nur für MSI-Installationen erforderlich). ■ Die Sicherheitseinstellungen des Browsers müssen den Download von ActiveX-Steuerelemente auf den Zielcomputer zulassen. Nach Abschluss der Installation kann die ursprüngliche Einstellung für die Sicherheitsstufe wiederhergestellt werden. ■ Die Systemanforderungen für das zu installierende Paket müssen erfüllt sein. ■ Der Benutzer muss am Computer mit den Berechtigungen angemeldet sein, die für das zu installierende Paket erforderlich sind. Sie benötigen Administratorrechte für die Installation von pcAnywhere.

Installations-Web-Server einrichten

Führen Sie zum Einrichten des Web-Servers die folgenden Schritte in der angegebenen Reihenfolge aus:

- Kopieren Sie die Installationsdateien auf den Web-Server.
- Konfigurieren Sie den Web-Server.

Installationsdateien auf den Web-Server kopieren

Sie müssen die Installationsdateien für die Unterstützung der webbasierten Verteilung in ein Verzeichnis auf dem Web-Server kopieren. Sie sollten auf dem Web-Server ein separates Verzeichnis für diese Dateien erstellen. Darüber hinaus müssen Sie die Installationsdateien (.exe oder .msi), die Sie zur Verfügung stellen möchten, kopieren.

Anschließend müssen Sie die Dateien "Start.htm" und "Files.ini" bearbeiten und den Speicherort und die Namen der Installationsdateien angeben.

Siehe "Verteilungsdateien anpassen" auf Seite 56.

So kopieren Sie die Installationsdateien auf den Web-Server:

1. Erstellen Sie auf dem Web-Server ein Verzeichnis für die Verteilungsdateien.
   Beispiel:
   Deploy
2. Kopieren Sie die Installationsdateien, die Sie für die Verteilung bereitstellen möchten, aus dem Ordner "Packages" auf der Symantec pcAnywhere-CD in den untergeordneten Ordner "Webinst" auf dem Web-Server.
   Beispiel:
   Deploy\Webinst\Webinst
3. Stellen Sie sicher, dass das Standarddokument für das virtuelle Verzeichnis "Default.htm" lautet.
   Siehe "Installations-Web-Server einrichten" auf Seite 52.

Es folgt ein Beispiel für die Ordnerstruktur auf dem Web-Server. Bei allen Dateien wird zwischen Groß- und Kleinschreibung unterschieden.

- Deploy\Webinst
  - brnotsup.htm
  - default.htm
  - intro.htm
  - logo.jpg
  - oscheck.htm
  - plnotsup.htm
  - readme.htm
  - start.htm
  - webinst.cab

- Deploy\Webinst\Webinst
  - files.ini
  - Launch.bat (nur für MSI-Installationen erforderlich)
  - Installationspakete
    Beispiel:
    Symantec pcAnywhere - Vollständiges Produkt.exe
    Symantec pcAnywhere - Nur Host (Netzwerk).msi

Virtuelles Verzeichnis auf dem Web-Server erstellen

Sie müssen den Web-Server konfigurieren, um ein virtuelles Verzeichnis zu erstellen.

So erstellen Sie ein virtuelles Verzeichnis auf einem Microsoft Internet Information Server oder Apache Web Server:

Das webbasierte Verteilungs-Tool unterstützt Microsoft Internet Information Server (IIS) oder Apache HTTP Web Server. Zum Erstellen eines virtuellen Verzeichnisses auf diesen Servern sind jeweils unterschiedliche Schritte auszuführen.

So erstellen Sie ein virtuelles Verzeichnis auf einem Microsoft Internet Information Server:

1. Führen Sie einen der folgenden Schritte aus, um den Internetdienste-Manager zu starten:
   - In IIS 4.0: Klicken Sie in der Windows-Taskleiste auf "Start > Programme > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internetdienste-Manager".
   - In IIS 5.0: Klicken Sie in der Windows-Taskleiste auf "Start > Programme > Verwaltung > Internetdienste-Manager".
2. Doppelklicken Sie auf das Web-Server-Symbol, um den Web-Server zu öffnen.
3. Klicken Sie mit der rechten Maustaste auf "Standardwebsite", und klicken Sie dann auf "Neu > Virtuelles Verzeichnis".
4. Klicken Sie auf "Weiter", um den Assistenten zum Erstellen virtueller Verzeichnisse zu starten.
5. Geben Sie in das Textfeld "Alias" einen Namen für das virtuelle Verzeichnis ein (z. B. "ClientInstall"), und klicken Sie dann auf "Weiter".

6. Geben Sie den Speicherort des Installationsordners ein (z. B. "C:\Client\Webinst"), und klicken Sie dann auf "Weiter".
7. Aktivieren Sie als Zugriffsberechtigungen die Option "Schreibgeschützt", und klicken Sie dann auf "Weiter".
8. Führen Sie einen der folgenden Schritte aus, um das Erstellen des virtuellen Verzeichnisses abzuschließen:
   - In IIS 4.0: Klicken Sie auf "Fertig stellen".
   - In IIS 5.0: Klicken Sie auf "Weiter" und dann auf "Fertig stellen".

So erstellen Sie ein virtuelles Verzeichnis auf einem Apache Web Server:

1. Öffnen Sie die Datei "Srm.conf" in einem Texteditor.
   Die Datei "Srm.conf" wird standardmäßig im Verzeichnis "C:\Programme\Apache Group\Apache\conf" installiert.
2. Geben Sie die folgenden fünf Zeilen am Ende der Datei "Srm.conf" ein:
   DirectoryIndex default.htm
   <VirtualHost 111.111.111.111>
   #ServerName Computername
   DocumentRoot "C:\Client\Webinst"
   </VirtualHost>

Für VirtualHost	Ersetzen Sie 111.111.111.111 durch die IP-Adresse des Computers, auf dem Apache HTTP Server installiert ist.
Für ServerName	Ersetzen Sie "Computername" durch den Namen des Servers.
Für DocumentRoot	Geben Sie den Ordner an, in den Sie die Webinstallationsdateien kopiert haben (z. B. "C:\Client\Webinst"). Für "DocumentRoot" sind doppelte Anführungszeichen erforderlich. Ohne die Anführungszeichen werden die Apache-Dienste möglicherweise nicht gestartet.

Verteilungsdateien anpassen

Sie müssen die folgenden Dateien bearbeiten, um Pakete mit Hilfe des webbasierten Verteilungs-Tools verteilen und installieren zu können:

- Start.htm: Enthält die Parameter für den Web-Server und den Pfad zu den Dateien, die installiert werden müssen.
  Die Datei ist im Stammverzeichnis des Verzeichnisses "Webinstall" gespeichert.
- Files.ini: Enthält die Dateinamensparameter für die Pakete und Dateien, die Sie verteilen und installieren möchten.
  Die Datei ist im Unterverzeichnis "Webinst" gespeichert.
- Launch.bat: Enthält die Befehlszeile, mit der die Paketinstallation gestartet wird.
  Die Datei ist im Unterverzeichnis "Webinst" gespeichert. Launch.bat ist nur für MSI-Installationen erforderlich.

Start.htm anpassen

Die Parameter in der Datei "Start.htm" enthalten Informationen zum Web-Server und zu den Speicherorten der Dateien, die installiert werden müssen. Die Konfigurationsparameter in Tabelle 3-2 befinden sich im unteren Abschnitt der Datei "Start.htm", innerhalb der <object>-Tags.

Tabelle 3-2 Konfigurationsparameter und -werte für "Start.htm"

Parameter	Wert
ServerName	Der Name des Servers, auf dem sich die Quelldateien für die Installation befinden. Sie können den Host-Namen, die IP-Adresse oder den NetBIOS-Namen verwenden. Die Quelldateien müssen auf einem HTTP-Web-Server abgelegt sein.
VirtualHomeDirectory	Das virtuelle Verzeichnis des HTTP-Servers, in dem die Quelldateien für die Installation gespeichert sind (z.B. "Deploy\Webinst").
ConfigFile	Der Name der Files.ini-Datei. Der Standardwert für diesen Parameter muss nicht geändert werden, es sei denn, die Datei "Files.ini" wurde von Ihnen umbenannt.
ProductFolderName	Das Unterverzeichnis, das die Quelldateien enthält, die lokal heruntergeladen werden müssen. Dieses Unterverzeichnis enthält das Paket sowie die Datei "Files.ini" (z.B. "Webinst").

Tabelle 3-2 Konfigurationsparameter und -werte für "Start.htm"

Parameter	Wert
MinDiskSpaceInMB	Die für den Festplattenspeicher geltenden Mindestanforderungen. Der Standardwert ist ausreichend.
ProductAbbreviation	Die für das Produkt verwendete Abkürzung. Der Standardwert ist ausreichend.

So passen Sie "Start.htm" an:

1. Öffnen Sie die Datei "Start.htm" in einem Texteditor.
2. Suchen Sie nach den <object>-Tags, und geben Sie die entsprechenden Werte ein.
   Siehe Tabelle 3-2, "Konfigurationsparameter und -werte für "Start.htm"," auf Seite 56.
3. Speichern Sie die Datei "Start.htm".

Files.ini für die Paketverteilung anpassen

Bearbeiten Sie die Datei "Files.ini", und fügen Sie den Namen der ausführbaren Paketdatei hinzu, die Sie verteilen möchten. Für eine MSI-Verteilung sind zusätzliche Informationen erforderlich.

Siehe "Files.ini für die MSI-Verteilung anpassen" auf Seite 58.

Sie können weitere Dateien hinzufügen, um die Verteilung von Anwendungen anderer Hersteller zu unterstützen.

So passen Sie die Datei "Files.ini" für die Paketverteilung an:

1. Öffnen Sie die Datei "Files.ini" in einem Texteditor.
2. Bearbeiten Sie im Abschnitt [General] die Zeile LaunchApplication= derart, dass auf die ausführbare Paketdatei verwiesen wird, die nach Abschluss des Downloads gestartet werden soll.
   Beispiel: LaunchApplication=Symantec pcAnywhere - Vollständiges Produkt.exe
3. Wenn Sie mehrere Dateien verteilen, bearbeiten Sie die Zeile FileCount=, und geben Sie die Anzahl der zu verteilenden Dateien an.
   Die Standardeinstellung lautet FileCount=1.

4 Bearbeiten Sie im Abschnitt [Files] die Zeile File1=, so dass auf den Namen des Pakets verwiesen wird, das Sie verteilen möchten.

   Beispiel: File1=Symantec pcAnywhere - Vollständiges Produkt.exe

   Lange Dateinamen werden unterstützt.

5 Fügen Sie für jede zusätzliche Datei eine neue Zeile "File*n*= *Dateiname*" hinzu, wobei "n" eine eindeutige Zahl und "Dateiname" den Namen der Datei darstellt.

6 Speichern Sie die Datei "Files.ini".

Files.ini für die MSI-Verteilung anpassen

Ändern Sie die Datei "Files.ini", um die Namen der .msi-Dateien hinzuzufügen, die Sie verteilen möchten. Für die MSI-Verteilung wird die Datei "Launch.bat" benötigt, die das Installationsprogramm startet. Sie müssen die Datei "Files.ini" so bearbeiten, dass darin auf die Datei "Launch.bat" verwiesen wird.

Siehe "Launch.bat anpassen" auf Seite 59.

Sie können weitere Dateien hinzufügen, um die Verteilung von Anwendungen anderer Hersteller zu unterstützen.

So passen Sie die Datei "Files.ini" für die MSI-Verteilung an:

1 Öffnen Sie die Datei "Files.ini" in einem Texteditor.

2 Bearbeiten Sie im Abschnitt [General] die Zeile LaunchApplication= derart, dass auf die Datei "Launch.bat" verwiesen wird.

   Beispiel: LaunchApplication=Launch.bat

   Damit wird nach Abschluss des Downloads die MSI-Installation gestartet. Zusätzlich müssen Sie die Datei "Launch.bat" bearbeiten und den Namen der .msi-Datei hinzufügen, die Sie verteilen möchten.

3 Bearbeiten Sie die Zeile FileCount=, und geben Sie die Anzahl der Dateien an, die Sie verteilen möchten.

   Für die MSI-Verteilung sind mindestens zwei Dateien erforderlich. In die Zeile FileCount= muss also mindestens die Zahl 2 eingegeben werden.

   Beispiel: FileCount=2

4 Bearbeiten Sie im Abschnitt [Files] die Zeile File1= derart, dass auf die Datei "Launch.bat" verwiesen wird.

   Beispiel: File1=Launch.bat

5 Löschen Sie das Semikolon vor der Zeile File2=, um den Eintrag nicht länger als Kommentar zu kennzeichnen.

6 Bearbeiten Sie die Zeile File2=, und geben Sie den Namen der .msi-Datei ein, die Sie verteilen möchten.

Beispiel: File2=Symantec pcAnywhere - Nur Host.msi

Lange Dateinamen werden unterstützt.

7 Fügen Sie für jede zusätzliche Datei eine neue Zeile "File*n*= *Dateiname*" hinzu, wobei "n" eine eindeutige Zahl und "Dateiname" den Namen der Datei darstellt.

8 Speichern Sie die Datei "Files.ini".

Launch.bat anpassen

Die Datei "Launch.bat" enthält das Befehlszeilenargument, mit dem eine MSI-Installation gestartet wird. Diese Datei ist nur für MSI-Installationen erforderlich.

Bearbeiten Sie die Datei "Launch.bat", und geben Sie die .msi-Datei an, die Sie verteilen möchten. In der Standarddatei für "Launch.bat" verweist der Pfad auf das Windows-Systemverzeichnis. Diese Befehlszeile ist für die MSI-Verteilung unter Windows 98/Me/NT erforderlich und stellt sicher, dass das System die für die Installation der .msi-Datei benötigte "msiexec.exe"-Datei findet.

Zusätzlich müssen Sie die Datei "Files.ini" so bearbeiten, dass darin auf die Datei "Launch.bat" verwiesen wird.

Siehe "Files.ini für die MSI-Verteilung anpassen" auf Seite 58.

Hinweis: Für die Installation von .msi-Dateien ist Windows Installer ab Version 2.0 erforderlich. Überprüfen Sie vor der Verteilung der Produktinstallation, ob der Zielcomputer die Systemanforderungen erfüllt.

Sie passen Sie "Launch.bat" an:

1 Öffnen Sie die Datei "Launch.bat" in einem Texteditor.

2 Stellen Sie sicher, dass folgende Befehlszeile in der Datei enthalten ist:
@SET PATH=%path%;%windir%\system

3 Bearbeiten Sie die Zeile "@msiexec -i Package.msi", und geben Sie für "Package.msi" den Name der .msi-Datei an, die Sie verteilen möchten.

Beispiel: @msiexec -i Symantec Packager - Nur Host.msi

Installation testen

Rufen Sie zum Testen der Installation die Website (z.B. <Ihre Website>/webinstall) auf, und klicken Sie auf "Installieren".

Beachten Sie etwaige Fehlermeldungen, falls die Installation fehlschlägt:

- Bei Problemen mit den Parametern in der Datei "Start.htm" wird eine Fehlermeldung angezeigt, die den Pfad zu den Dateien enthält, auf die die webbasierte Installation zuzugreifen versucht. Überprüfen Sie, ob der Pfad korrekt angegeben ist.
- Bei Problemen mit der Datei "Files.ini" (Fehler "Datei nicht gefunden") müssen Sie den Wert "File1=" mit dem tatsächlichen Namen der Paketdatei vergleichen.
- Vergewissern Sie sich, dass keine anderen Einträge während der Bearbeitung geändert wurden.

Benutzer über den Speicherort zum Herunterladen informieren

Benutzern können Sie per E-Mail Anweisungen senden, wie sie das Paket, das Sie verteilen möchten, herunterladen können.

Für die Installation eines pcAnywhere-Installationsprogramms muss auf den Computern der Benutzer Internet Explorer ab Version 4.0 vorhanden sein. Für die Sicherheitsstufe von Internet Explorer für das lokale Intranet muss "Mittel" ausgewählt sein, damit Symantec ActiveX-Steuerelemente auf den Client heruntergeladen werden können. Nach Abschluss der Installation kann die ursprüngliche Einstellung für die Sicherheitsstufe wiederhergestellt werden.

Stellen Sie sicher, dass die Benutzer die Systemanforderungen kennen und über die erforderlichen Administratorrechte für die zu installierenden Produkte verfügen. Beispielsweise benötigen Benutzer für die Installation von pcAnywhere unter Windows NT/2000/XP Administratorrechte auf ihrem eigenen Computer und müssen als Administrator angemeldet sein. Für die Installation von Symantec pcAnywhere ist außerdem Internet Explorer ab Version 5.5 SP2 erforderlich.

Falls das Paket den Clientcomputer nach Abschluss der Installation neu startet, sollten die Benutzer aufgefordert werden, ihre Arbeit zu speichern und ihre Anwendungen zu schließen, bevor sie mit der Installation beginnen. Beispielsweise wird bei einer Installation ohne Ausgabe auf Computern unter Windows 98 der Computer nach Abschluss der Installation neu gestartet.

Fügen Sie in Ihrer E-Mail wie folgt einen URL hinzu, der auf die Clientinstallation verweist:

- Für Internet Information Server:

  http://Servername/Virtuelles_Basisverzeichnis/Webinst/

  Dabei steht "Servername" für den Namen des webbasierten Servers, "Virtuelles_Basisverzeichnis" für den Namen des Alias, den Sie erstellt haben, und "Webinst" für den Ordner, den Sie auf dem Web-Server erstellt haben (z.B. "http://Servername/ClientInstall/Webinst/").

- Für Apache Web Server:

  http://Servername/Webinst/

  Dabei steht "Servername" für den Namen des Computers, auf dem Apache HTTP Server installiert ist. Die IP-Adresse des Servercomputers kann anstelle von "Servername" verwendet werden.

Verteilen von pcAnywhere mit Hilfe von SMS 2.0

Für die Verteilung von pcAnywhere mit Microsoft Systems Management Server (SMS) 2.0) werden die folgenden Komponenten benötigt:

- pcAnywhere-Installationsdatei: Ein Installationspaket oder eine angepasste Produktinstallation, das bzw. die mit Symantec Packager erstellt wurde. Dabei ist die Verwendung als selbstextrahierende ausführbare Datei (.exe) oder als .msi-Datei möglich.
- SMS-Paket: Eine Sammlung von Installationsquellen und -paketen, die für die Inventarisierung und Installation von Softwareprogrammen auf SMS-Clients verwendet werden. Als SMS-Paket ist jeder Softwaretyp zulässig, der die Installation über SMS unterstützt.
- PDF-Datei (Package Definition File): Eine SMS-spezifische Informationsdatei, die von SMS für das Erstellen und Verteilen von SMS-Paketen verwendet wird. Die mit pcAnywhere gelieferte Standard-PDF heißt "pcAnywhere.pdf".

Mindestanforderungen für die SMS-Installation

Für die Verteilung von pcAnywhere mit SMS werden die folgenden Komponenten benötigt:

- Windows NT 4.0-Server mit Service Pack 5 oder höher
- SQL-Server ab Version 6.5
- SMS 2.0 mit Service Pack 1 oder Service Pack 2 (empfohlen)
- Symantec Packager ab Version 1.0 mit angepassten Paketen für die Verteilung

Alle Verteilungsclients müssen entweder der gleichen Domäne angehören wie der SMS-Verteilungsserver, oder dem SMS-Server müssen Verwaltungsrechte auf allen Clients eingeräumt werden, indem zwischen den Domänen eine Vertrauensstellung mit den entsprechenden Zugriffsrechten eingerichtet wird.

SMS 2.0 muss auf Windows NT 4.0 mit Service Pack 5 oder höher installiert sein. Es wird empfohlen, das SMS Service Pack 2 oder höher von Microsoft zu beziehen. Auf der Microsoft-Website http://www.microsoft.com/sms finden Sie die neuesten Informationen zu den SMS-Updates und schrittweise Anleitungen für die Installation der Service Packs.

pcAnywhere mit SMS verteilen

Die Verteilung mit SMS umfasst vier Schritte:

- PDF-Datei vorbereiten
- SMS-Verteilungspaket erstellen
- Verteilungspunkte zuordnen
- Paket ankündigen

PDF-Datei vorbereiten

pcAnywhere wird mit einer Standard-PDF-Datei (pcAnywhere.pdf) ausgeliefert. Diese Datei kann so bearbeitet werden, dass sie jedes mit Symantec Packager erstellte Paket verarbeiten kann.

Führen Sie einen der folgenden Schritte aus, um die mitgelieferte PDF-Datei zu verwenden, ohne sie zu ändern:

- Ändern Sie für .exe-basierte Pakete den Namen des pcAnywhere-Pakets, das Sie verwenden möchten, in "Package.exe".
- Ändern Sie für .msi-basierte Pakete den Namen des pcAnywhere-Pakets, das Sie verwenden möchten, in "Package.msi".

Weitere Informationen zur Anpassung der PDF-Datei finden Sie in Ihrer SMS-Dokumentation.

Die folgenden Werte dürfen in der mitgelieferten PDF-Datei weder gelöscht noch geändert werden:

- AfterRunning=ProgramRestart
- CanRunWhen=UserLoggedOn
- AdminRightsRequired=TRUE

SMS-Verteilungspaket erstellen

Für jede pcAnywhere-Installation, die Sie auf den Client-Computern ausführen wollen, muss ein SMS-Paket erstellt und eine Verteilung konfiguriert werden.

So erstellen Sie ein SMS-Verteilungspaket:

1. Erstellen Sie mit Symantec Packager eine .msi-Produktinstallationsdatei bzw. eine .exe-Paketinstallationsdatei oder verwenden Sie eines der vorkonfigurierten pcAnywhere-Pakete, die zusammen mit pcAnywhere ausgeliefert werden.
2. Klicken Sie in der SMS Administrator-Konsole mit der rechten Maustaste auf "Pakete", und klicken Sie dann auf "Neu > Paket aus einer Definition".
3. Wenn Sie im Fenster "Willkommen beim Assistenten für die Erstellung eines Pakets aus einer Definition" zur Eingabe des Namens einer Paketdatei aufgefordert werden, klicken Sie auf "Durchsuchen", um nach der Datei "pcAnywhere.pdf" zu suchen.

   Der Standardpfad lautet: C:\Programme\Symantec\pcAnywhere\CMS.
4. Klicken Sie auf "Öffnen".

   Der "Assistent für die Erstellung eines Pakets aus einer Definition" zeigt die pcAnywhere-Paketdefinition an.
5. Klicken Sie auf "Weiter".
6. Klicken Sie auf "Dateien immer aus einem Quellverzeichnis abrufen".

   Vorsicht: Wählen Sie "Dieses Paket enthält keine Dateien" nicht aus.
7. Klicken Sie auf "Durchsuchen", um nach dem Ordner zu suchen, der das pcAnywhere-Paket enthält, das Sie mit Symantec Packager erstellt haben (oder ein mitgeliefertes, vorkonfiguriertes Paket).

   Der "Assistent für die Erstellung eines Pakets aus einer Definition" erstellt mit Hilfe dieses Ordners einen Zeiger auf das pcAnywhere-Paket.
8. Nachdem Sie den "Assistenten für die Erstellung eines Pakets aus einer Definition" ausgeführt haben, wird ein pcAnywhere-Paket in der SMS Administrator-Konsole angezeigt.

Verteilungspunkte zuordnen

Nachdem Sie das SMS-Paket erstellt haben, müssen Sie einen Verteilungspunkt für das Paket angeben.

So ordnen Sie Verteilungspunkte zu:

1. Klicken Sie mit der rechten Maustaste auf "Verteilungspunkte", und klicken Sie anschließend auf "Neu > Verteilungspunkt".
2. Aktivieren Sie die Verteilungspunkte, an die Sie das Paket verteilen wollen.
3. Klicken Sie auf "Fertig stellen", um die Ausführung des Verteilungspunkt-Assistenten zu beenden.

Paket ankündigen

Um die pcAnywhere-Installation an die Clients zu senden, muss für eine bzw. mehrere Paketinstallationen eine Ankündigung erstellt werden.

So kündigen Sie das Paket an:

1. Klicken Sie mit der rechten Maustaste auf "Ankündigungen", und klicken Sie dann auf "Neu > Ankündigung".
2. Wählen Sie das Paket aus, das Sie ankündigen möchten.
3. Weisen Sie der Ankündigung einen aussagefähigen Namen zu.
4. Wählen Sie im Dropdown-Menü eine der folgenden Installationen aus:
   - Windows Me/Windows 2000 für die Verteilung an Windows Me- und Windows 2000-Clients, die MSI-basierte Installationen unterstützen.
   - Windows 9x/Windows NT für die Verteilung des pcAnywhere-Pakets an Windows 9x- und Windows NT-Clients.
5. Klicken Sie auf "Durchsuchen", und wählen Sie die Sammlung aus, an die Sie die Installationsankündigung senden möchten.
6. Konfigurieren Sie den Zeitplan, die Anforderungen und relevanten Sicherheitsrechte des Pakets.

Nachdem die Ankündigung fertig gestellt ist, sollte pcAnywhere mit der Verteilung an alle ausgewählten Clients beginnen.

Hinweis: Bei Ankündigungen, die mit dem EXE-basierten Installationsprogramm erstellt wurden, müssen die Benutzer Informationen eingeben. Die Benutzer werden aufgefordert, ein temporäres Verzeichnis auf dem lokalen Client-Computer auszuwählen, um die Installationsdateien zu extrahieren. Nachdem die Dateien extrahiert sind, werden die Benutzer aufgefordert, auf "Ja" zu klicken, damit das Setup-Programm mit der Installation von pcAnywhere beginnt. Die Benutzer sollten die temporären Setup-Dateien nach Abschluss der Installation löschen.

Windows NT/2000/XP-Anmeldeskripts

In einer Windows-Domäne können pcAnywhere-Pakete mit Hilfe von Anmeldeskripts auf Windows-Clients verteilt werden. Hierfür müssen drei Schritte ausgeführt werden:

- Einrichten des Servers
- Erstellen des Anmeldeskripts
- Testen des Anmeldeskripts

Windows NT/2000/XP-Benutzer müssen über lokale Administratorrechte auf ihren Computern verfügen, um das pcAnywhere-Paket installieren zu können.

Server einrichten

Der Server muss so konfiguriert sein, dass das Speichern von pcAnywhere-Paketen und das Implementieren von Anmeldeskripts möglich ist. Für die Durchführung dieser Aufgaben benötigen Sie Administratorrechte für die Domäne.

So richten Sie den Server ein:

1. Erstellen Sie auf dem Server einen Ordner mit der Bezeichnung PCAHOME.
2. Geben Sie den Ordner frei, und verwenden Sie als Standardfreigabenamen für den Ordner PCAHOME.
3. Stellen Sie die Zugriffsrechte für diese Freigabe so ein, dass alle Benutzer Lesezugriff besitzen.
4. Kopieren Sie das pcAnywhere-Paket in die PCAHOME-Freigabe.

Anmeldeskript erstellen

Sie können pcAnywhere-Pakete mit Hilfe des weiter unten aufgeführten Beispielanmeldeskripts an Windows NT/2000/XP-Clients verteilen. Das Skript ist eine einfache Stapeldatei, mit der das pcAnywhere-Paket auf die Arbeitsstation kopiert, die Installation des pcAnywhere-Pakets gestartet und die Installationsdateien nach Abschluss der Installation gelöscht werden.

In den folgenden Beispielen wird von Standard-Installationsordnern ausgegangen. Diese Ordner können nach Bedarf bearbeitet werden, damit sie in Ihrer Arbeitsumgebung funktionieren.

```
@echo off
setlocal

REM ***** Package Variable -- Change to name of pcA Package *****
Set Package=Package.MSI

REM ***** EXE or MSI Variable -- Change to package type (MSI or EXE)
*****
Set PkgType=MSI

Rem ***** File Server Name Variable *****
Rem ***** Change to server containing the pcA Package *****
Set FSName=\\2KServer

REM ***** Maps a drive to the network share *****
net use z: %FSName%\PCAHOME

REM ***** Checks for pcA in default folder
If exist c:\progra~1\Symant~1\pcanyw~1\anywhere.bin GOTO End

REM ***** Creates a folder in the Temp dir, and copies the package
*****
C:
CD %TEMP%
MD pcapkg
CD pcapkg
Z:
COPY %Package% C:

REM ***** Launch Package Installation *****
C:
IF %PkgType% == MSI msiexec -i %Package%
IF %PkgType% == EXE %Package%

REM ***** Cleanup *****
del %Package%
CD ..
rd pcapkg
Net Use Z: /DELETE

:End
endlocal
```

Anmeldeskript testen

Testen Sie das fertig gestellte Skript auf ein oder zwei Arbeitsstationen, bevor Sie es für alle Benutzer einrichten. Windows NT/2000/XP-Benutzer müssen über lokale Administratorrechte auf ihren Computern verfügen, um das pcAnywhere-Paket installieren zu können.

NetWare-Anmeldeskripts

In einem Novell NetWare-Netzwerk können pcAnywhere-Pakete mit Hilfe von Anmeldeskripts auf Windows-Clients verteilt werden. Hierfür müssen drei Schritte ausgeführt werden:

- Einrichten des Servers
- Erstellen des Anmeldeskripts
- Testen des Anmeldeskripts

Windows NT/2000/XP-Benutzer müssen über lokale Administratorrechte auf ihren Computern verfügen, um das pcAnywhere-Paket installieren zu können.

Server einrichten

Der Server muss so konfiguriert sein, dass das Speichern von pcAnywhere-Paketen und das Implementieren von Anmeldeskripts möglich ist. Für diese Schritte benötigen Sie Administratorrechte.

So richten Sie den Novell NetWare-Server ein:

1. Ordnen Sie Laufwerk Z: Volume SYS: zu.

   Wenn Sie einen anderen Laufwerksbuchstaben verwenden, müssen Sie den entsprechenden Laufwerksbuchstaben mit den folgenden Arbeitsschritten ersetzen.
2. Erstellen Sie im Ordner Z:\LOGIN einen Ordner mit der Bezeichnung PCA.
3. Erstellen Sie eine Gruppe mit der Bezeichnung PCA_Users.

   Die Gruppe PCA_Users sollte im Standardkontext für Server enthalten sein, die sowohl NDS- als auch Bindery-Anmeldungen verarbeiten. Wenn der Server nur NDS-Anmeldungen verarbeitet, sollte diese Gruppe in einen Kontext eingefügt werden, der in der auf dem Server gespeicherten NDS-Partition installiert ist.
4. Erteilen Sie der Gruppe PCA_Users Leserechte für den PCA-Ordner.
5. Kopieren Sie das pcAnywhere-Paket in den PCA-Ordner.

Anmeldeskript erstellen

Verwenden Sie für die verteilte Installation von pcAnywhere das Anmeldeskript und die Verteilungsstapeldatei, das/die im folgenden Beispiel beschrieben werden. Das Skript erstellt die korrekten Laufwerkszuordnungen für die lokale Arbeitsstation und startet die Stapeldatei für die Verteilung. Die Stapeldatei installiert das pcAnywhere-Paket und löscht nach Abschluss des Vorgangs die Installationsdateien.

In den folgenden Beispielen wird von Standard-Installationsordnern ausgegangen. Diese Ordner können nach Bedarf bearbeitet werden, damit sie in Ihrer Arbeitsumgebung funktionieren.

NetWare-Anmeldeskript

```
REM ***** Default mappings *****
MAP *1:=SYS:

REM ***** Maps a drive to the network share *****
MAP Z:=SYS:LOGIN\PCA

REM ***** Launches the deployment batch file *****
#Cmd /c z:\deploy.bat

Beenden
```

Installations-Batch-Datei

```
@echo off
setlocal

REM ***** Package Variable -- Change to name of pcA Package *****
Set Package=Package.MSI

REM ***** EXE or MSI Variable -- Change to package type (MSI or EXE)
*****
Set PkgType=MSI

REM ***** Checks for pcA in default folder *****
If exist c:\progra~1\Symant~1\pcanyw~1\anywhere.bin GOTO End

REM ***** Creates a folder in the Temp dir, and copies the package
*****
C:
CD %TEMP%
MD pcapkg
CD pcapkg
Z:
COPY %Package% c:
```

```
REM ***** Launches Package Installation *****
C:
IF %PkgType% == MSI msiexec -i %Package%
IF %PkgType% == EXE %Package%

REM ***** Cleanup *****
del %Package%
CD ..
rd pcapkg

:End
endlocal
```

Anmeldeskript testen

Testen Sie das fertig gestellte Skript auf ein oder zwei Arbeitsstationen, bevor Sie es für alle Benutzer einrichten. Windows NT/2000-Benutzer müssen über lokale Administratorrechte auf ihren Computern verfügen, um das pcAnywhere-Paket installieren zu können.

Kapitel 4

Zentrales Management

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zum zentralen Management
- Fernverwaltung von pcAnywhere-Hosts
- Integration in Microsoft Systems Management Server (SMS)
- Informationen zu Microsoft Distributed Component Object Model (DCOM)
- Informationen zur zentralen Protokollierung

Informationen zum zentralen Management

Symantec pcAnywhere enthält das pcAnywhere Host-Administrator-Tool, das Ihnen die Fernverwaltung mehrerer pcAnywhere-Hosts im Netzwerk ermöglicht. Das pcAnywhere Host-Administrator-Tool ist ein Microsoft Management Console (MMC) Snap-In, für dessen Ausführung MMC benötigt wird. MMC ist auf der Symantec pcAnywhere-CD im Ordner "Tools" abgelegt.

Symantec pcAnywhere unterstützt zudem die Integration mit Microsoft Systems Management Server.

Siehe "Integration in Microsoft Systems Management Server (SMS)" auf Seite 81.

Symantec pcAnywhere unterstützt die zentrale Ereignisprotokollierung mit Hilfe des pcAnywhere Host-Administrators oder eines SNMP-Monitors.

Siehe "Informationen zur zentralen Protokollierung" auf Seite 85.

Fernverwaltung von pcAnywhere-Hosts

Der pcAnywhere Host-Administrator ist ein Administrator-Tool für die Fernverwaltung von Hosts im Netzwerk. Mit dem pcAnywhere Host-Administrator können Sie folgende Aufgaben ausführen:

- per Fernverbindung pcAnywhere-Hosts im Netzwerk starten, stoppen und eine Verbindung dazu herstellen;
- Konfigurationsgruppen erstellen, um mehrere Arbeitsstationen im Netzwerk über eine Fernverbindung zu verwalten und zu konfigurieren;
- pcAnywhere-Konfigurationsdateien, einschließlich Optionsgruppen sowie Host-, Remote- und Anruferdateien, gleichzeitig auf mehrere Arbeitsstationen im Netzwerk verteilen.

pcAnywhere Host-Administrator-Tool installieren

Das pcAnywhere Host-Administrator-Tool ist als benutzerdefinierte Installationsoption im Rahmen der vollständigen Produktinstallation verfügbar. Für das pcAnywhere Host-Administrator-Tool muss Windows NT/2000/XP installiert sein.

Installieren Sie das Host-Administrator-Tool wie im Folgenden beschrieben nach der Installation von pcAnywhere.

So installieren Sie das Host-Administrator-Tool:

1. Klicken Sie in der Windows-Taskleiste auf "Start > Einstellungen > Systemsteuerung".
2. Doppelklicken Sie im Fenster der Systemsteuerung auf "Software".
3. Klicken Sie im Fenster "Software" auf "Symantec pcAnywhere".
4. Klicken Sie auf "Ändern".
5. Klicken Sie im Fenster zum Ändern oder Entfernen von Symantec pcAnywhere auf "Weiter".
6. Klicken Sie im Fenster "Programmverwaltung" auf "Ändern".
7. Klicken Sie auf "Weiter".
8. Klicken Sie im Fenster "Angepasstes Setup" unter "pcAnywhere-Tools" auf den Pfeil nach unten neben "Host-Administrator", und klicken Sie dann auf "Dieses Feature wird auf eine lokale Festplatte installiert".
9. Klicken Sie auf den Pfeil nach unten neben "Host-Administrator-Agent", und klicken Sie dann auf "Dieses Feature wird auf eine lokale Festplatte installiert".

   Der Host-Administrator-Agent wird für die Fernverwaltung von pcAnywhere mit Hilfe der Distributed Component Object Management (DCOM)-Technologie benötigt.
10. Klicken Sie auf "Weiter".
11. Um das Programmsymbol zum Windows-Desktop hinzuzufügen, aktivieren Sie "pcAnywhere Host-Administrator".
12. Klicken Sie auf "Installieren".
13. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Installationsvorgang fortzusetzen. Klicken Sie nach Abschluss der Installation auf "Fertig stellen".
14. Falls für Ihren Computer die Aktualisierung von Systemdateien erforderlich ist, werden Sie aufgefordert, den Computer neu zu starten. Dies ist notwendig, um den fehlerfreien Betrieb sicherzustellen.

Host-Administrator-Snap-In zu MMC hinzufügen

Mit Microsoft Management Console (MMC) können Sie Administrator-Tools zentral ausführen und verwalten. Während der Installation können Sie das pcAnywhere Host-Administrator-Tool als Snap-In in MMC integrieren.

MMC ist im Lieferumfang des Betriebssystems Windows 2000/XP enthalten. Falls die MMC-Software nicht auf Ihrem Computer installiert ist, können Sie sie von der Symantec pcAnywhere-CD installieren.

So integrieren Sie das Host-Administrator-Snap-In in MMC:

1. Klicken Sie in der Windows-Taskleiste auf "Start > Programme > pcAnywhere Host-Administrator".
2. Klicken Sie zum Starten von MMC in der Windows-Taskleiste auf "Start > Ausführen", und geben Sie **mmc** ein.
3. Klicken Sie im Konsolenmenü auf "Snap-In hinzufügen/entfernen".
4. Klicken Sie im Fenster "Snap-In hinzufügen/entfernen" auf der Registerkarte "Eigenständig" auf "Hinzufügen".
5. Klicken Sie im Fenster "Eigenständiges Snap-In hinzufügen" auf "pcAnywhere Host-Administrator".
6. Klicken Sie auf "Hinzufügen".
7. Klicken Sie auf "Schließen".
8. Klicken Sie im Fenster "Snap-In hinzufügen/entfernen" auf "OK".

Konfigurationsgruppen erstellen

Für die Fernverwaltung und Fernkonfiguration von Computern mit Hilfe der pcAnywhere Host-Administrator-Konsole müssen Sie eine Konfigurationsgruppe erstellen und die Computer dann zu dieser Gruppe hinzufügen.

Siehe "Computer zu einer Konfigurationsgruppe hinzufügen" auf Seite 75.

Wenn Sie MMC verwenden, ist die pcAnywhere Host-Administrator-Konsole unter "Konsolenstamm" aufgeführt.

Weitere Informationen finden Sie in der MMC-Dokumentation.

So erstellen Sie eine Konfigurationsgruppe:

1. Klicken Sie im Konsolenfenster im linken Fensterbereich unter "pcAnywhere Host-Administrator" mit der rechten Maustaste auf "Konfigurationsgruppen", und klicken Sie dann auf "Neu > Konfigurationsgruppe".
2. Geben Sie einen Namen für die Gruppe ein.
3. Klicken Sie auf "OK".

Computer zu einer Konfigurationsgruppe hinzufügen

Nachdem Sie eine Konfigurationsgruppe erstellt haben, müssen Sie die Computer hinzufügen, die Sie per Fernverbindung verwalten möchten. Im Konsolenfenster werden die Domänen und Arbeitsgruppen Ihres Netzwerks aufgeführt.

So fügen Sie Computer zu einer Konfigurationsgruppe hinzu:

1. Wechseln Sie im Konsolenfenster im linken Fensterbereich zu den Computern, die Sie hinzufügen möchten, z. B. Microsoft Windows-Netzwerk.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf das System mit den Computern, die Sie hinzufügen möchten, und klicken Sie dann auf "Systeme zu Konfigurationsgruppen hinzufügen".
3. Wählen Sie im Fenster "Systeme zu Konfigurationsgruppen hinzufügen" die Computer aus, die Sie hinzufügen möchten.
4. Wählen Sie unter "Wählen Sie die Zielgruppe(n) aus" die Konfigurationsgruppe aus, zu der Sie die Computer hinzufügen möchten.
5. Klicken Sie auf "OK".

Administrator-Host- und Remote-Verbindungsobjekte konfigurieren

Vor der Verwendung des pcAnywhere Host-Administrators zur Fernverwaltung der Hosts im Netzwerk müssen Sie zunächst die Administrator-Host- und Remote-Verbindungsobjekte konfigurieren. Diese Dateien enthalten die Verbindungs- und Sicherheitseinstellungen, die für die Unterstützung von Verbindungen zwischen der pcAnywhere Host-Administrator-Konsole und den Host-Computern, die Sie verwalten möchten, erforderlich sind.

Symantec pcAnywhere enthält die folgenden vorkonfigurierten Host- und Remote-Verbindungsobjekte, die als Vorlage verwendet werden können:

- Admin.bhf: Host-Vorlage für die Host-Computer, die per Fernverbindung verwaltet werden sollen.

  Um mit dieser Vorlage eine Host-Sitzung zu starten, müssen Sie die Anruferinformationen konfigurieren. Symantec pcAnywhere benötigt für alle Host-Sitzungen einen Benutzernamen und ein Kennwort.

  Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

- Admin11.chf: Host-Administrator-Vorlage für den Computer, für den Hosts per Fernverbindung verwaltet werden sollen.

Sie können diese Vorlagen in pcAnywhere ändern oder neue Administratorobjekte erstellen. Die Vorlagendateien sind im folgenden Verzeichnis gespeichert:

\Programme\Symantec\pcAnywhere\CMS

Neues Administrator-Remote-Objekt erstellen

Das Administrator-Remote-Verbindungsobjekt enthält die Verbindungs- und Sicherheitsinformationen, die für die Verbindung mit einem Host-Computer von der pcAnywhere Host-Administrator-Konsole aus erforderlich sind. Diese Datei hat die Dateierweiterung .chf.

Diese Datei können Sie zum CMS-Ordner hinzufügen, um sie im pcAnywhere Host-Administrator zu verwenden, oder in ein Installationspaket einbinden.

So erstellen Sie ein neues Administrator-Remote-Objekt:

1. Klicken Sie in pcAnywhere-Manager auf der linken Navigationsleiste auf "Remotes".
2. Klicken Sie im Menü "Datei" auf "Neu > Objekt > Weitere Optionen".
3. Wählen Sie im Remote-Eigenschaftenfenster auf der Registerkarte "Verbindungsinformationen" eines der folgenden Netzwerkprotokolle aus:
   - TCP/IP
   - SPX
   - NetBIOS
4. Konfigurieren Sie im Remote-Eigenschaftenfenster weitere Einstellungen, die Sie verwenden möchten.
5. Wenn Sie alle gewünschten Einstellungen geändert haben, klicken Sie auf "OK".
   Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
6. Klicken Sie in pcAnywhere-Manager im rechten Fensterbereich unter "Remotes" mit der rechten Maustaste auf das soeben erstellte Remote-Verbindungsobjekt, und klicken Sie dann auf "Umbenennen".
7. Geben Sie einen Namen ein.
   Beispiel:
   Admin11

Neue Administrator-Host-Objekte erstellen

Die Administrator-Host-Verbindung enthält die Verbindungs- und Sicherheitsinformationen, die dem Remote-Administrator die Verbindung von der pcAnywhere Host-Administrator-Konsole aus ermöglichen. Ein Anruferobjekt muss vorhanden sein.

Diese Datei hat die Dateierweiterung .bhf. Anruferdateien haben die Dateierweiterung .cif. Diese Dateien können Sie zum CMS-Ordner hinzufügen, um sie im pcAnywhere Host-Administrator zu verwenden, oder in ein Installationspaket einbinden.

So erstellen Sie ein neues Administrator-Host-Objekt:

1. Klicken Sie in pcAnywhere-Manager auf der linken Navigationsleiste auf "Hosts".
2. Klicken Sie im Menü "Datei" auf "Neu > Objekt > Weitere Optionen".
3. Wählen Sie im Host-Eigenschaftenfenster auf der Registerkarte "Verbindungsinformationen" eines der folgenden Netzwerkprotokolle aus:
   - TCP/IP
   - SPX
   - NetBIOS
4. Wählen Sie auf der Registerkarte "Anrufer" den gewünschten Authentifizierungstyp aus.
5. Klicken Sie unter "Anruferliste" auf das Symbol "Neues Objekt".
6. Geben Sie im Anrufer-Eigenschaftenfenster die Anmeldeinformationen für die Benutzer an, die eine Verbindung zum Host-Computer herstellen können, und klicken Sie dann auf "OK".

   Für alle Host-Verbindungen ist ein Benutzername und ein Kennwort erforderlich. Sie können weitere Einstellungen konfigurieren, wie z. B. Zugriffsrechte.

   Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
7. Konfigurieren Sie im Host-Eigenschaftenfenster weitere Einstellungen, die Sie verwenden möchten, und klicken Sie dann auf "OK".

   Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
8. Klicken Sie in pcAnywhere-Manager im rechten Fensterbereich unter "Hosts" mit der rechten Maustaste auf das soeben erstellte Host-Verbindungsobjekt, und klicken Sie dann auf "Umbenennen".
9. Geben Sie einen Namen ein.

   Beispiel:

   Admin

Host-Objekt im pcAnywhere Host-Administrator konfigurieren

Mit dem pcAnywhere Host-Administrator-Tool können Sie ein Host-Objekt erstellen und an die Host-Computer in der Konfigurationsgruppe verteilen. In Symantec pcAnywhere müssen Sie ein Anmeldekonto für Benutzer einrichten, die eine Verbindung zu Ihrem Computer herstellen, und eine Authentifizierungsmethode zur Überprüfung ihrer Identität auswählen.

So konfigurieren Sie ein Host-Objekt im pcAnywhere Host-Administrator:

1. Klicken Sie im Konsolenfenster im linken Fensterbereich unter "pcAnywhere Host-Administrator" auf das Pluszeichen neben "Konfigurationsgruppen", um diese zu erweitern.
2. Klicken Sie unter dem Namen der Konfigurationsgruppe, zu der Sie ein Host-Objekt hinzufügen möchten, mit der rechten Maustaste auf Verbindungsobjekte, und klicken Sie dann auf "Neu > Host-Modus".
3. Geben Sie einen Namen für dieses Verbindungsobjekt ein.
4. Klicken Sie auf "OK".
5. Konfigurieren Sie das Host-Verbindungsobjekt, und geben Sie Anruferinformationen sowie andere benötigte Informationen an.

   Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

pcAnywhere-Konfigurationsdateien verteilen

Mit dem pcAnywhere Host-Administrator-Tool können Sie pcAnywhere-Konfigurationsdateien, wie z. B. Host-Verbindungsobjekte, von der pcAnywhere Host-Administrator-Konsole aus an die Host-Computer in Ihrer Konfigurationsgruppe verteilen.

Der Host-Computer muss auf eine Verbindung warten.

So verteilen Sie pcAnywhere-Konfigurationsdateien:

1. Klicken Sie in der pcAnywhere Host-Administrator-Konsole im linken Fensterbereich unter "pcAnywhere Host-Administrator" auf das Pluszeichen neben "Konfigurationsgruppen", um diese zu erweitern.
2. Klicken Sie unter "Konfigurationsgruppen" mit der rechten Maustaste auf die Konfigurationsgruppe, an die Sie die Dateien senden möchten, und klicken Sie dann auf "pcAnywhere-Dateien verteilen".
3. Wählen Sie im Fenster "pcAnywhere-Dateien verteilen" die Computer aus, an die Sie die Datei verteilen möchten.

4 Wählen Sie die Datei aus, die Sie verteilen möchten.

5 Klicken Sie auf "OK".

Hosts in einer Konfigurationsgruppe verwalten

Nachdem Sie die Computer in Ihrer Konfigurationsgruppe konfiguriert haben, können Sie mit der pcAnywhere Host-Administrator-Konsole jeden verwalteten Host in der Gruppe starten, stoppen oder eine Verbindung mit diesem Host in der Gruppe herstellen.

So verwalten Sie Host in einer Konfigurationsgruppe:

1 Klicken Sie in der pcAnywhere Host-Administrator-Konsole im linken Fensterbereich unter "pcAnywhere Host-Administrator" auf das Pluszeichen neben "Konfigurationsgruppen", um diese zu erweitern.

2 Klicken Sie unter "Konfigurationsgruppen" auf das Pluszeichen neben dem Namen der Konfigurationsgruppe, um diese zu erweitern.

3 Klicken Sie unter "Systeme" mit der rechten Maustaste auf den Computer, den Sie verwalten möchten, und klicken Sie anschließend auf "Alle Tasks".

4 Wählen Sie eine der folgenden Optionen aus:

- Bestimmten Host starten: Startet eine Host-Sitzung auf dem ausgewählten Host-Computer.
- Admin-Host starten: Startet eine Host-Sitzung auf dem Host-Administrator-Computer.
- Letzten Host starten: Startet eine Host-Sitzung auf dem Computer, auf dem Sie zuletzt eine Host-Sitzung gestartet haben.
- Host stoppen: Bricht die Host-Sitzung ab und trennt alle aktiven Sitzungen auf dem Host.
- Verbinden mit Admin-Host: Stellt mit den in der Remote-Datei "admin11.chf" angegebenen Einstellungen eine Verbindung zum Host-Administrator-Computer her.
- Admin-Host konfigurieren: Konfiguriert die Einstellungen auf dem Host-Administrator-Computer neu.
- Aktivitätslogbuch abrufen: Ruft das Aktivitätslogbuch vom Remote-Computer ab.

Integration in Microsoft Systems Management Server (SMS)

Symantec pcAnywhere unterstützt die Integration in Microsoft Systems Management Server (SMS). SMS ist ein skalierbares Änderungs- und Konfigurationsverwaltungssystem für Microsoft Windows-basierte Computer und Server.

Symantec pcAnywhere liefert die erforderlichen Unterstützungsdateien für die Integration in SMS. Diese Dateien sind nur auf der Symantec pcAnywhere Corporate-CD vorhanden.

Paketdefinitionsdatei in SMS importieren

Symantec pcAnywhere enthält eine Paketdefinitionsdatei (pcAnywhere.pdf) mit Programmeinstellungen und sonstigen produktspezifischen Informationen, die für die Integration in SMS erforderlich sind. Sie müssen diese Datei in SMS importieren.

Diese Datei ist im Ordner "Tools" auf der Installations-CD gespeichert.

So importieren Sie die Paketdefinitionsdatei in SMS:

1. Legen Sie die Symantec pcAnywhere-CD in das CD-ROM-Laufwerk ein.
2. Klicken Sie in pcAnywhere-Installationsfenster auf "Tools".
   Eine HTML-Seite wird geöffnet.
3. Klicken Sie im Web-Browser-Fenster unter "Tools anderer Hersteller" auf "Microsoft System Management Server (SMS)".
4. Klicken Sie unter "Microsoft System Management Server (SMS)" auf "pcAnywhere.pdf-Datei speichern".
5. Wählen Sie im Explorer-Fenster den Speicherort aus, an dem Sie die Datei speichern möchten.
6. Starten Sie SMS auf dem BackOffice-Server.
7. Importieren Sie in SMS Administrator die Datei "pcAnywhere.pdf" mit Hilfe des Importdienstprogramms.
8. Kopieren Sie den Inhalt aller sieben Disketten im Verzeichnis "\installs\pcanywhere\pca32full\cd\disk1" in ein Verzeichnis auf dem Server.

Weitere Informationen zur Installation und Verteilung von Anwendungen mit Hilfe eines BackOffice-Servers finden Sie in der SMS-Dokumentation.

Informationen zu Microsoft Distributed Component Object Model (DCOM)

Symantec pcAnywhere nutzt die DCOM-Technologie von Microsoft für jede Art von Punkt-zu-Punkt-Kommunikation bei der Durchführung von Remote-Management-Aufgaben. DCOM wird im pcAnywhere Host-Administrator-Tool und bei der SMS-Integration verwendet.

DCOM läuft unter einer Vielzahl von Netzwerkprotokollen und versucht standardmäßig, Verbindungen mit allen installierten Protokollen herzustellen. Nach dem Verbindungsaufbau mit dem Netzwerk überprüft DCOM mit der Windows NT-Authentifizierung die erforderlichen Zugriffsrechte. Beispielsweise kann ein Systemadministrator mit den entsprechenden Zugriffsrechten von jedem Standort aus Verwaltungsaufgaben für einen gesperrten pcAnywhere-Host ausführen.

Um sicherzustellen, dass die Windows NT-Authentifizierung für die DCOM-Verwaltungsaufgaben von pcAnywhere verwendet werden, sollten die pcAnywhere-Verbindungsobjekte für die gleiche Domäne oder auf einer vertrauten Domäne konfiguriert werden.

Windows NT/2000/XP für DCOM konfigurieren

Um pcAnywhere unter Windows NT/2000/XP mit Hilfe eines zentralen Verwaltungs-Tools zu konfigurieren und zu steuern, müssen die folgenden Systemanforderungen erfüllt sein:

- Der Administrator muss als Domänenverwalter angemeldet sein.
- Der Computer des Administrators und der des Clients müssen sich in der gleichen Domäne befinden.

Für die Windows NT-Standardkonfiguration müssen alle Management-Aktivitäten in der Windows NT-Domäne authentifiziert werden.

Windows 98/Me für DCOM konfigurieren

Um pcAnywhere unter Windows 98/XP mit Hilfe eines zentralen Verwaltungs-Tools zu konfigurieren und zu steuern, müssen die folgenden Systemanforderungen erfüllt sein:

- Der Windows 98/Me-Client muss bei der gleichen Windows NT-Domäne wie der Administrator angemeldet sein.
- Der Domänenname und der Arbeitsgruppenname auf dem Computer unter Windows 98/Me müssen identisch sein.
- Der Computer unter Windows 98/Me muss mit Zugriffsrechten der Benutzerebene konfiguriert sein. Diese Zugriffsrechte werden benötigt, um die DCOM-Sicherheitseinstellungen bei der Ausführung des Programms "dcomcnfg.exe" anpassen zu können.
- Die Datei- und Druckerfreigabe für Microsoft Windows-Netzwerke sollte auf dem Computer unter Windows 98/Me installiert und aktiviert sein.

DCOM-Einstellungen bearbeiten

Symantec pcAnywhere konfiguriert DCOM während der Installation. Die Standardeinstellungen sollten ausreichen, um den normalen Betrieb der pcAnywhere-Management-Anwendungen zu ermöglichen und ein ausreichendes Sicherheitsniveau zu gewährleisten. Administratoren können jedoch die Standardsicherheitseinstellungen in DCOM ändern, um den Zugriff auf ein System zuzulassen oder zu verweigern.

Für die Bearbeitung von DCOM-Sicherheitseinstellungen auf einem verwalteten Computer müssen Sie möglicherweise die DCOM-Einstellungen auf dem Administrator-Computer anpassen. Vergewissern Sie sich, dass alle verwalteten Computer bei der gleichen Windows NT-Domäne oder auf vertrauten Domänen authentifiziert werden.

Wenn eine Administratorverbindung zu einem Remote-Computer hergestellt wird, versucht die zentrale Management-Software die Identität des Benutzers, der die Verbindung herstellt, anzunehmen. Wenn der Benutzer nicht mit Administratorrechten angemeldet ist, schlägt der Identitätswechsel fehl.

Um die Sicherheit weiterhin zu gewährleisten, kann ein Anrufer ohne Administratorrechte keine Administratorfunktionen ausführen und hat nur die Zugriffsrechte, über die er verfügt, wenn er sich direkt bei dem Computer anmeldet.

Um Verbindungsprobleme aufgrund von Zugriffsverweigerungsfehlern zu vermeiden, prüfen Sie mit Hilfe des Dienstprogramms "dcomcnfg.exe" die Sicherheitseinstellungen für den Client. Bearbeiten Sie die Standardsicherheit, und fügen Sie nur die Domänenbenutzer oder Administratoren hinzu, die auf diesen Host zugreifen dürfen

Weitere Informationen finden Sie nach Bedarf in der Online-Dokumentation zu DCOMCNFG.EX

So ändern Sie DCOM-Einstellungen unter Windows NT:

- Führen Sie eine der folgenden Aktionen aus:
  Öffnen Sie unter Windows NT/2000/XP den Ordner "\WinNT\System32", und führen Sie "dcomcnfg.exe" aus.
  Öffnen Sie unter Windows 98/Me den Ordner "\Windows\System", und führen Sie "dcomcnfg.exe" aus.

AwShim

AwShim ist der Management-Adapter zwischen pcAnywhere und der zentralen Management-Integration. Das pcAnywhere Host-Administrator-Tool verwendet AwShim für das Starten und Stoppen von Host- und Remote-Sitzungen. Für jede Aktion können bestimmte Host- oder Remote-Konfigurationsdateien zugewiesen werden.

AwShim verwendet die folgenden Parameter:

- -A Aktion
- -B Bhf-Dateiname
- -C Chf-Dateiname
- -H Host-Name, auf dem die Aktion ausgeführt werden soll
- -R Remote-Computer, mit dem eine Verbindung hergestellt werden soll

Unterstützte Aktionen mit dem Parameter -A:

- STARTHOST
- STARTREMOTE
- STOPHOST

Die Parameter -B und -C definieren die Objekte "Host-Modus" und "Host-PC anrufen", die sich im CMS-Ordner des pcAnywhere-Verzeichnisses befinden.

Der Parameter -H gibt den Namen oder die Adresse des Host-Computer an, auf dem die Aktion ausgeführt wird.

Der Parameter -R wird nur zusammen mit STARTREMOTE verwendet, um den Namen des Host-Computers anzugeben, mit dem der Remote-Server eine Verbindung herstellt. Wenn ein Remote gestartet wird, werden mit Ausnahme der Host-Computer-Adresse alle in der CHF-Datei angegebenen Verbindungsparameter verwendet. Die Adresse muss mit dem Parameter -R angegeben werden.

Wenn ein kennwortgeschütztes Verbindungsobjekt auf einem verwalteten Computer ausgeführt wird, wird die Aufforderung zur Kennworteingabe nur auf dem verwalteten Computer angezeigt. Auf dem Computer, von dem aus der Administrator die Aktion gestartet hat, dagegen nicht.

Informationen zur zentralen Protokollierung

Sicherheit, Zuständigkeiten und Protokollierung sind wichtige Bestandteile jeder verteilten Computerumgebung. Symantec pcAnywhere verfügt über ein erweitertes Logdienstprogramm, das die zentrale Ereignisprotokollierung unterstützt. Der Administrator kann Loginformationen von jedem pcAnywhere-Host im Netzwerk sammeln und auf einem sicheren, zentralen Server speichern.

Das pcAnywhere Host-Administrator-Tool kann Protokolldateien von einem Host-Computer im Netzwerk abrufen und lokal anzeigen und verarbeiten.

Symantec pcAnywhere unterstützt die Logfunktion auch auf einer SNMP-Konsole (Simple Network Management Protocol). Mit SNMP werden SNMPv1-Traps an eine kompatible Konsole gesendet, die diese Informationen aufzeichnet. Symantec pcAnywhere stellt eine Management Information Base (MIB) mit den von pcAnywhere generierten SNMP-Ereignissen zur Verfügung.

Leistung mit Hilfe von SNMP-Traps überwachen

SNMP ist ein Protokoll für die Netzwerküberwachung, das Aktivitäten auf Netzwerkgeräten, wie z. B. Adaptern, Routern und Hubs, überwacht und protokolliert.

Diese Informationen können dann an jede Management-Konsole gesendet werden, die SNMP-Traps unterstützt, wie z. B. MMC oder SMS. Die Ereigniskonsole bietet normalerweise die Möglichkeit, Aktionen in Abhängigkeit vom eingehenden SNMP-Trap und den darin enthaltenen Variablen zu automatisieren. Die Funktionen der automatisierten Aktion, die normalerweise als Regel oder Aktion bezeichnet wird, sind je nach zentralem Management-Tool unterschiedlich. Mit den meisten können Sie jedes Programm starten, das in der Befehlszeile ausgeführt werden kann.

Siehe "pcAnywhere MIB-Datei" auf Seite 86.

So überwachen Sie die Leistung mit Hilfe von SNMP-Traps:

1. Klicken Sie in pcAnywhere-Manager im Menü "Bearbeiten" auf "Voreinstellungen".
2. Aktivieren Sie im pcAnywhere-Fenster "Optionen" auf der Registerkarte "Ereignisprotokollierung" das Kontrollkästchen "SNMP-Traps aktivieren".
   Um diese Registerkarte anzuzeigen, führen Sie mit Hilfe des Pfeils nach links bzw. rechts einen Bildlauf in der Registerkartenliste durch.
3. Klicken Sie auf "Hinzufügen", um den Computer anzugeben, der die Protokollierungsinformationen erhalten soll.
4. Geben Sie im Fenster "Ziel für SNMP-Traps" eine IP-Adresse ein.
   Wiederholen Sie diese Schritte für jeden Computer, den Sie hinzufügen möchten.
5. Klicken Sie auf "OK".
6. Wählen Sie die Ereignisse aus, die Sie protokollieren möchten.
   Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.
7. Klicken Sie auf "OK".

pcAnywhere MIB-Datei

Die pcAnywhere MIB-Datei definiert die SNMP-Traps, die pcAnywhere generieren kann. Verwenden Sie die pcAnywhere MIB-Datei als Hilfsmittel, um automatische Reaktionen auf pcAnywhere-Ereignisse zu definieren, die im Netzwerk auftreten.

Die pcAnywhere MIB-Datei befindet sich im folgenden Verzeichnis:

\Programme\Symantec\pcAnywhere\CMS\pca_trap.mib

```
--
--  pcAnywhere MIB Definitions (pcAnywhere 11.0)
--  Copyright 1999, 2000, 2003 Symantec Corporation.
--

PCA-Alert-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
        enterprises
              FROM RFC1155-SMI
    OBJECT-TYPE
          FROM RFC-1212
    TRAP-TYPE
              FROM RFC-1215
        DisplayString
              FROM RFC1213-MIB;


symantec   OBJECT IDENTIFIER ::= { enterprises 393 }
pcanywhere OBJECT IDENTIFIER ::= { symantec 100 }

-- pcAnywhere version 9x information --
pcaversionnineOBJECT IDENTIFIER ::= { pcanywhere 9 }

PcaHost  OBJECT IDENTIFIER ::= { pcaversionnine 1 }
PcaRemote OBJECT IDENTIFIER ::= { pcaversionnine 2 }
PcaFileXfer OBJECT IDENTIFIER ::= { pcaversionnine 3 }
PcaGateway OBJECT IDENTIFIER ::= { pcaversionnine 4 }
PcaMonitor   OBJECT IDENTIFIER ::= { pcaversionnine 5 }
PcaInstall OBJECT IDENTIFIER ::= { pcaversionnine 6 }
PcaReset OBJECT IDENTIFIER ::= { pcaversionnine 7 }
PcaLDAP  OBJECT IDENTIFIER ::= { pcaversionnine 8 }

-- PcaObject declares variable definitions
PcaObject  OBJECT IDENTIFIER ::= { pcaversionnine 9 }


-- pcA version 10 specific information:
pcaversiontenOBJECT IDENTIFIER ::= { pcanywhere 10 }
PcaHostV10 OBJECT IDENTIFIER ::= { pcaversionten 1 }
PcaObjectV10OBJECT IDENTIFIER ::= { pcaversionten 2 }
```

```
-- pcA version 11 specific information:
pcaversionelevenOBJECT IDENTIFIER ::= { pcanywhere 11 }
PcaRemoteManagementOBJECT IDENTIFIER ::= { pcaversioneleven 1 }

-- Pca Alert Objects - These are not able to be queried, however
they are
-- used for the trap variables we will bind to specific traps.

HostComputerName  OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS  read-only
              STATUS    optional
              DESCRIPTION
                        "The computer that is running the PCA Host"
              ::= { PcaObject 1 }

RemoteComputerName  OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                       "The computer that is running the PCA Remote"
              ::= { PcaObject 2 }

CallerName    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..128))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The name of the remote caller."
              ::= { PcaObject 3 }
```

```
HostConnectionObject    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The name of the connection object used to
start the PCA Host"
              ::= { PcaObject 4 }

RemoteConnectionObject    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The name of the connection object used to
start the PCA Remote"
              ::= { PcaObject 5 }

XferFiles OBJECT-TYPE
              SYNTAXINTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
            "Number of files transferred by file transfer"
              ::= { PcaObject 6 }

XferBytes OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
            "Number of bytes transferred by this file transfer
operation"
              ::= { PcaObject 7 }
```

```
-- Possible values for XferOperation are:
--  0. Sent
--  1. Recieved
--  2. Folder Created
--  3. Delete
--  4. Copy
--  5. Move
--  6. Rename

XferOperation OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "The operation last performed by file transfer"
              ::= { PcaObject 8 }

XferVirusFlag OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "This is the file transfer virus flag."
              ::= { PcaObject 9 }

XferSourceFile    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The name of the source file in a file
transfer operation"
              ::= { PcaObject 10 }
```

```
XferDestFile    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The name of the destination file in a file
transfer operation"
              ::= { PcaObject 11 }

HostEncryptionLevel  OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "The desired encryption level of the PCA Host"
              ::= { PcaObject 12 }

RemoteEncryptionLevel OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "The desired encryption level of the PCA Remote"
              ::= { PcaObject 13 }

HostEndedReason OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "The reason a PCA Host was terminated"
              ::= { PcaObject 14 }
```

```
-- Possible reasons for HostEndedReason, these would occur on a
session end.
--   0. Remote Logged Off
--   1. Host Ended Session
--   2. Connection Lost
--   3. Remote canceled
--   4. Inactivity timeout
--   5. Usage timeout
--   6. Host reboot
--   7. Remote reboot
--   8. Login failed
--   9. Invalid password
--  10. Encryption failure
--  11. Device Failure


-- If the Host Stopped for any reason, HostEndedReason will contain
-- one of the following negative results
--  -1. Device type is unavailable
--  -2. Couldn't Sync State
--  -3. cm_open failed
--  -4. cm_attach failed
--  -5. cm_stat failed
--  -6. Generic failure to get a connection
--  -7. The host was busy
--  -8. The user cancelled the operation
--  -9. Network host name not found
-- -10. Unable to load a modem configuration
-- -11. Asked to change an invalid parameter
-- -12. Unable to process a modem script
-- -13. Modem responded with unknown response
-- -14. Modem could not answer
-- -15. Couldn't sync to modem speed
-- -16. No answer from the modem
-- -17. Gateway error
-- -18. ISDN call rejected
```

```
-- -19. ISDN no phone line
-- -20. ISDN line out of order
-- -21. ISDN invalid destination address
-- -22. ISDN destination number changed
-- -23. ISDN outgoing calls unauthorized
-- -24. ISDN dest not authorized to accept calls
-- -25. Could not update LDAP with status

DeviceType OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "This represents the type of device in which a connection
was made."
              ::= { PcaObject 15 }

-- Available Device Types
--  0. Null Device
--  1. TTY
--  2. Printer
--  3. 8250
--  4. NCSI
--  5. IPX
--  6. NetBios
--  7. INT 14
--  8. AppleTalk
--  9. IPX Driver for MACs with NAS
-- 10. Telebit ACS device
-- 11. Banyan
-- 12. SPX
-- 13. TCP/IP
-- 14. TAPI
-- 15. CAPI
```

```
XFerFailedFlag OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
           "This flag will be set if a file transfer event had
failed."
              ::= { PcaObject 16 }

EncryptionErrorMessage    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "Encryption error message"
              ::= { PcaObject 17 }

P3SerialNumber OBJECT-TYPE
              SYNTAX  DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                       "Processor serial number"
              ::= { PcaObject 18 }

SystemName OBJECT-TYPE
              SYNTAX  DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                       "Name of the system generating the event."
              ::= { PcaObject 19 }


-- pca Version 10 - Newly added Host events --
```

```
FileAccessReason OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
            "How a file was accessed"
              ::= { PcaObjectV10 1 }

-- Possible values for FileAccessReason are:
--  0. File Create
--  1. File Read
--  2. File Delete
--  3. File Edit

SourceFile    OBJECT-TYPE
              SYNTAX    DisplayString (SIZE (0..255))
              ACCESS    read-only
              STATUS    optional
              DESCRIPTION
                        "The file that was accessed"
              ::= { PcaObjectV10 2 }

IPAddressOBJECT-TYPE
               SYNTAXDisplayString (SIZE (0..255))
               ACCESS  read-only
               STATUS  optional
               DESCRIPTION
               "IP Address generating event"
              ::= { PcaObjectV10 3 }
```

```
CommandLineOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "A Command Line was executed from the command prompt"
               ::= { PcaRemoteManagement 1 }
SystemFileNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The name of the system file that was changed"
               ::= { PcaRemoteManagement 2 }
SystemStateOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "System State generating event"
               ::= { PcaRemoteManagement 3 }
ApplicationNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The name of the application removed"
               ::= { PcaRemoteManagement 4 }
ProcessEventOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "ProcessEvent generating event"
               ::= { PcaRemoteManagement 5 }
```

```
ProcessNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The name of the process which handles the event"
               ::= { PcaRemoteManagement 6 }
ServiceStateOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "Service State generating event"
               ::= { PcaRemoteManagement 7 }
ServiceNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The name of the service that handles the event"
               ::= { PcaRemoteManagement 8 }
ServiceDisplayNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The service display name"
               ::= { PcaRemoteManagement 9 }
ServiceDescriptionOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The service description"
               ::= { PcaRemoteManagement 10 }
```

```
LogOnTypeOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "Service log on type"
               ::= { PcaRemoteManagement 11 }
ServiceInteractWithDesktopOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "Service Interact With Desktop generating event"
               ::= { PcaRemoteManagement 12 }
RegistryChangeOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "Registry Change generating event"
               ::= { PcaRemoteManagement 13 }
RegKeyNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The registry key name"
               ::= { PcaRemoteManagement 14 }
RegValueNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The registry value name"
               ::= { PcaRemoteManagement 15 }
```

```
RegValueDataOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The registry value data"
               ::= { PcaRemoteManagement 16 }
RegFileNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The registry file name"
               ::= { PcaRemoteManagement 17 }
RegNewKeyNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The new registry key name"
               ::= { PcaRemoteManagement 18 }
RegNewValueNameOBJECT-TYPE
                SYNTAXDisplayString (SIZE (0..255))
                ACCESS  read-only
                STATUS  optional
                DESCRIPTION
                "The new registry value name"
               ::= { PcaRemoteManagement 19 }
```

```
-----------------------------------------------------------------
-- Version 9 Trap Definitions
-----------------------------------------------------------------
-- Pca Host Alert Traps
PcaHostStarted   TRAP-TYPE
                 ENTERPRISE  PcaHost
                 VARIABLES   {
                              DeviceType,
                              HostConnectionObject,
                              P3SerialNumber,
                              SystemName
                             }
                 DESCRIPTION "PCA Host was started"
                 ::= 1

PcaHostEndSession TRAP-TYPE
                 ENTERPRISE  PcaHost
                 VARIABLES   {
                             HostEndedReason,
                         SystemName
                             }
                 DESCRIPTION "PCA Host has shut down"
                 ::= 2

PcaHostAbnormalEnd   TRAP-TYPE
                 ENTERPRISE  PcaHost
                 DESCRIPTION "PCA Host has shut down abnormally"
                 ::= 3
```

```
PcaHostConnFailDeviceError   TRAP-TYPE
                ENTERPRISE  PcaHost
                VARIABLES   {
                            DeviceType,
                          SystemName
                            }
                DESCRIPTION "PCA Host connection failed - device
error"
                ::= 4

PcaHostStopped   TRAP-TYPE
                ENTERPRISE  PcaHost
                VARIABLES   {
                            HostEndedReason,
                          SystemName
                            }
                DESCRIPTION "PCA Host was stopped"
                ::= 5

PcaHostInSession   TRAP-TYPE
                ENTERPRISE  PcaHost
                VARIABLES   {
                            RemoteComputerName,
                           CallerName,
                          SystemName
                            }
                DESCRIPTION "PCA Host is in session"
                ::= 6
```

```
PcaHostConnFailAccessDenied   TRAP-TYPE
                 ENTERPRISE  PcaHost
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Host connection failed - access
denied"
                 ::= 7

PcaHostConnFailEncrypt   TRAP-TYPE
                 ENTERPRISE  PcaHost
                 VARIABLES   {
                             EncryptionErrorMessage,
                          SystemName
                             }
               DESCRIPTION "PCA Host connection failed - encryption
error"
                 ::= 8

PcaHostUnsecuredHostStarted   TRAP-TYPE
                 ENTERPRISE  PcaHost
                 VARIABLES   {
                             HostConnectionObject,
                          SystemName
                             }
                 DESCRIPTION "Unsecure launch of PCA Host"
                 ::= 9

PcaHostRebooting   TRAP-TYPE
                 ENTERPRISE  PcaHost
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Host rebooting the system"
                 ::= 10
```

```
PcaHostLockingWorkstation TRAP-TYPE
                ENTERPRISE  PcaHost
                VARIABLES {
                          SystemName
                          }
                DESCRIPTION "PCA Host locking workstation"
                ::= 11

PcaHostLoggingOffUser TRAP-TYPE
                ENTERPRISE  PcaHost
                VARIABLES {
                          SystemName
                          }
                DESCRIPTION "PCA Host is logging off the current
user"
                ::= 12

-------------------------------------------------------------------
-- pcA Version 10.0 New host traps --
-------------------------------------------------------------------

PcaHostFileAccess TRAP-TYPE
                ENTERPRISE  PcaHostV10
                VARIABLES {
                             HostComputerName,
                             RemoteComputerName,
                             SourceFile,
                             FileAccessReason
                          }
                DESCRIPTION "Host file access"
                ::= 1
```

```
PcaHostExeLaunch TRAP-TYPE
                ENTERPRISE  PcaHostV10
                VARIABLES {
                            HostComputerName,
                            RemoteComputerName,
                            SourceFile
                          }
                DESCRIPTION "Host executable launch"
                ::= 2

PcaConnPortScanned TRAP-TYPE
                   ENTERPRISE PcaHostV10
                   VARIABLES{
                              IPAddress
                              }
                   DESCRIPTION "Port Scanned"
                   ::= 3

PcaConnRapsScanned TRAP-TYPE
               ENTERPRISE     PcaHostV10
                VARIABLES {
                            IPAddress
                          }
                DESCRIPTION "Raps Scanned"
                ::= 4

PcaConnFailedRestrictedIP TRAP-TYPE
               ENTERPRISE     PcaHostV10
                VARIABLES {
                            IPAddress
                          }
                DESCRIPTION "Restricted IP"
                ::= 5
```

```
PcaConnFailedSerialMismatch TRAP-TYPE
              ENTERPRISEPcaHostV10
               VARIABLES {
                            IPAddress,
                            RemoteComputerName
                          }
               DESCRIPTION "Serial Mismatch"
               ::= 6

PcaAuthWarningTRAP-TYPE
                  ENTERPRISE  PcaHostV10
                 VARIABLES{
                              CallerName
                            }
                 DESCRIPTION "Authentication Warning - Weak
Password"
                 ::= 7
-----------------------------------------------------------------
PCA Remote Generated Traps
-----------------------------------------------------------------

PcaRemoteStarted   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                            DeviceType,
                            RemoteConnectionObject,
                            P3SerialNumber,
                            SystemName
                           }
                DESCRIPTION "PCA Remote was started"
                ::= 1
```

```
PcaRemoteInSession   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                            HostComputerName,
                         SystemName
                            }
                DESCRIPTION "PCA Remote is in session"
                ::= 2

PcaRemoteEndSession   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                         SystemName
                            }
                DESCRIPTION "PCA Remote has ended the session"
                ::= 3

PcaRemoteAbnormalEndSession   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                         SystemName
                            }
                DESCRIPTION "PCA Remote has ended the session
abnormally"
                ::= 4

PcaRemoteConnFailDeviceError   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                            DeviceType,
                         SystemName
                            }
               DESCRIPTION "PCA Remote connection failure - device
error"
                ::= 5
```

```
PcaRemoteConnFailHostBusy   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                          SystemName
                             }
                DESCRIPTION "PCA Remote connection failure - host
busy"
                ::= 6

PcaRemoteConnFailHostNotFound   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                          SystemName
                             }
                DESCRIPTION "PCA Remote connection failure - host
not found"
                ::= 7

PcaRemoteConnFailBadPassword   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                          SystemName
                             }
                DESCRIPTION "PCA Remote connection failure - bad
password"
                ::= 8

PcaRemoteConnFailEncryption   TRAP-TYPE
                ENTERPRISE  PcaRemote
                VARIABLES   {
                             EncryptionErrorMessage,
                          SystemName
                             }
                DESCRIPTION "PCA Remote connection failure -
encryption error"
                ::= 9
```

```
-----------------------------------------------------------------
-- PCA File Transfer Generated Traps
-----------------------------------------------------------------

PcaFileXferStarted   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
                VARIABLES   {
                            HostComputerName,
                            RemoteComputerName,
                         SystemName
                            }
                DESCRIPTION "PCA File Transfer started"
                ::= 1

PcaFileXferEnded   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
                VARIABLES   {
                         SystemName
                            }
                DESCRIPTION "PCA File Transfer ended"
                ::= 2

PcaFileXferAbnormalEnd   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
                VARIABLES   {
                            HostComputerName,
                            RemoteComputerName,
                         SystemName
                            }
                DESCRIPTION "PCA File Transfer ended abnormally"
                ::= 3
```

```
PcaFileXferOperationCancelled   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
               VARIABLES {
                         SystemName
                         }
                DESCRIPTION "PCA File Transfer operation cancelled"
                ::= 4

PcaFileXferOperation   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
                VARIABLES   {
                         XferOperation,
                         XferSourceFile,
                         XferDestFile,
                         XferBytes,
                         XferVirusFlag,
                         XferFailedFlag,
                         SystemName
                            }
                DESCRIPTION "PCA File Transfer detailed operation
notice"
                ::= 5

PcaFileXferVirusFound   TRAP-TYPE
                ENTERPRISE  PcaFileXfer
                VARIABLES   {
                      XferSourceFile,
                         SystemName
                            }
                DESCRIPTION "PCA File Transfer has detected a
virus."
                ::= 6
```

```
-----------------------------------------------------------------
-- PCA Version 11 - Remote Management Events
-----------------------------------------------------------------
RMCmdPrmptCmdLine  TRAP-TYPE
                    ENTERPRISE  PcaRemoteManagement
                   VARIABLES {
                              CommandLine
                              }
                    DESCRIPTION "Command Prompt - Command Line"
                    ::= 1

RMSysFileChanges  TRAP-TYPE
                    ENTERPRISE  PcaRemoteManagement
                   VARIABLES {
                              SystemFileName
                              }
                    DESCRIPTION "System File Changes"
                    ::= 2

RMSysStateChanges  TRAP-TYPE
                    ENTERPRISE  PcaRemoteManagement
                   VARIABLES {
                              SystemState
                              }
                    DESCRIPTION "System State Changes"
                    ::= 3

RMUninstallApp  TRAP-TYPE
                    ENTERPRISE  PcaRemoteManagement
                   VARIABLES {
                              ApplicationName
                              }
                    DESCRIPTION "Uninstall Application"
                    ::= 4
```

```
RMProcessChanges  TRAP-TYPE
                   ENTERPRISE  PcaRemoteManagement
                  VARIABLES {
                            ProcessEvent,
                            ProcessName
                            }
                   DESCRIPTION "Process Changes"
                   ::= 5

RMServiceStateChanges  TRAP-TYPE
                   ENTERPRISE  PcaRemoteManagement
                  VARIABLES {
                            ServiceState,
                            ServiceName
                            }
                   DESCRIPTION "Service State Changes"
                   ::= 6

RMServiceCfgChanges  TRAP-TYPE
                   ENTERPRISE  PcaRemoteManagement
                  VARIABLES {
                            ServiceName,
                            ServiceDisplayName,
                            ServiceDescription,
                            LogOnType,
                            ServiceInteractWithDesktop
                            }
                   DESCRIPTION "Service Configuration Changes"
                   ::= 7
```

```
RMRegistryChanges  TRAP-TYPE
                 ENTERPRISE  PcaRemoteManagement
                VARIABLES {
                          RegistryChange,
                          RegKeyName,
                          RegValueName,
                          RegValueData,
                          RegFileName,
                          RegNewKeyName,
                          RegNewValueName
                          }
                 DESCRIPTION "Registry Changes"
                 ::= 8

-------------------------------------------------------------------
-- The remaining pcAnywhere SNMP Traps are not yet implemented
-- PCA Monitor Traps
-------------------------------------------------------------------

PcaMonitorFullProductNotInstalled   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Full product is
not installed"
                 ::= 1

PcaMonitorHostNotInstalled   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Host is not
installed"
                 ::= 2
```

```
PcaMonitorRemoteNotInstalled   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Remote is not
installed"
                 ::= 3

PcaMonitorHostNotWaiting   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Host is not
waiting for a connection"
                 ::= 4

PcaMonitorHostNotAutoStart   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Host is not set
to auto start"
                 ::= 5

PcaMonitorHostNotWaitingOnDialup   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - The PCA Host is not
waiting on a dialup"
                 ::= 6
```

```
PcaMonitorHostLanOnlyNotInstalled   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                DESCRIPTION "PCA Monitor - The PCA Host LAN only is
not installed"
                 ::= 7

PcaMonitorLiveUpdateNotRun   TRAP-TYPE
                 ENTERPRISE  PcaMonitor
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - Live Update was not run
on this host"
                 ::= 8

-------------------------------------------------------------------
-- Reset Events - these events are defined so that when generated by
the monitor they
-- can be used to clear the status of previously generated events.
-------------------------------------------------------------------

PcaResetNotInstalledReset   TRAP-TYPE
                 ENTERPRISE  PcaReset
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - Reset install traps"
                 ::= 1
```

```
PcaResetHostNotWaitingReset   TRAP-TYPE
                 ENTERPRISE  PcaReset
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - Reset Host not waiting
traps"
                 ::= 2

PcaResetHostNotAutoStartReset   TRAP-TYPE
                 ENTERPRISE  PcaReset
                VARIABLES {
                          SystemName
                          }
               DESCRIPTION "PCA Monitor - Reset Host not auto start
traps"
                 ::= 3

PcaResetHostWaitingOnDialupReset   TRAP-TYPE
                 ENTERPRISE  PcaReset
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Monitor - Reset Host waiting on
dialup traps"
                 ::= 4

PcaResetLiveUpdateNotRunReset   TRAP-TYPE
                 ENTERPRISE  PcaReset
                VARIABLES {
                          SystemName
                          }
               DESCRIPTION "PCA Monitor - Reset Live Update not run
traps"
                 ::= 5
```

```
-------------------------------------------------------------------
-- PCA Install Traps
-------------------------------------------------------------------

PcaInstallRebootRequired  TRAP-TYPE
                 ENTERPRISE  PcaInstall
                VARIABLES {
                          SystemName
                          }
                 DESCRIPTION "PCA Install - A reboot is required"
                 ::= 1


END
```

Kapitel 5

Integrieren von pcAnywhere in Verzeichnisdienste

In diesem Kapitel werden folgende Themen behandelt:

- Verzeichnisdienste
- Überblick über das LDAP Informational Model
- Verzeichnisdienste und pcAnywhere
- Konfigurieren der Verzeichnisserver
- Konfigurieren von pcAnywhere für die Verwendung von Verzeichnisdiensten

Verzeichnisdienste

Die Funktion "Verzeichnisdienste" in pcAnywhere ist ein Beispiel für eine LDAP (Lightweight Directory Access Protocol) Client-Anwendung zum Speichern und Abrufen von Benutzerinformationen. Sie ermöglicht ein leichteres Suchen nach Host-Computern, die auf eine Verbindung im Internet oder einem Intranet warten.

Die Verwendung von Verzeichnisdiensten mit pcAnywhere hat den Vorteil, dass die Geschwindigkeit gesteigert wird. Wenn Sie eine Remote-Verbindung starten wird das Netzwerk normalerweise nach wartenden pcAnywhere-Hosts durchsucht. Dieser Vorgang kann sich als zeitaufwendig erweisen, und die Ergebnisse können in Abhängigkeit von der Größe des Netzwerks und je nachdem, ob sich der Host in einem anderen Teilnetz befindet, unterschiedlich ausfallen. LDAP-registrierte Hosts stellen Ergebnisse zu Remote-Abfragen sofort zur Verfügung.

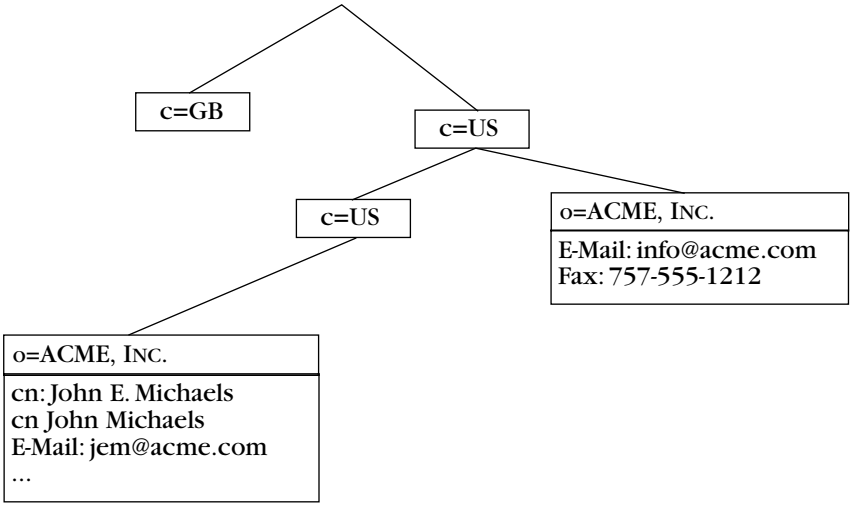
Überblick über das LDAP Informational Model

Das LDAP-Verzeichnis speichert Informationen in einer hierarchischen Baumstruktur, die mit einem Dateisystem mit Unterverzeichnissen und Dateien vergleichbar ist. Jedes Objekt im Verzeichnis wird als Eintrag bezeichnet. Bei Einträgen kann es sich um Container oder um Blatteinträge handeln.

Container sind Einträge, die wiederum andere Einträge enthalten können, während Blatteinträge die "Endpunkte" des Verzeichnisbaums darstellen. Container- und Blatteinträge stellen die Struktur einer Organisation dar, indem Einträge für Länder, Organisationseinheiten und Benutzer der verschiedenen Organisationsbereiche erstellt werden.

In dem in Abbildung 5-1 gezeigten Beispiel befinden sich an der Spitze des Verzeichnisbaums Einträge, die Länder repräsentieren. Darunter befinden sich Einträge für Bundesstaaten oder nationale Organisationen. Und darunter gibt es wiederum Einträge für Benutzer, Organisationseinheiten, Drucker oder sonstige Informationen.

Abbildung 5-1 Beispiel einer hierarchischen LDAP-Baumstruktur



Mit LDAP können für jeden Eintrag Attribute gespeichert werden, um weitere Informationen zu dem Eintrag bereitzustellen, wie beispielsweise den Namen, die E-Mail-Adresse, die Telefonnummer oder die Position des Benutzers. Jeder Eintrag kann mehrere Werte für das gleiche Attribut aufweisen.

Die für einen Eintrag zulässigen Attribute werden durch die zugehörige Objektklasse bestimmt. Ein LDAP-Server verfügt über eine Liste aller bekannten Objektklassen. Administratoren können neue Objektklassen hinzufügen und vorhandene Objektklassen bearbeiten, damit Client-Anwendungen bestimmte Attributtypen speichern können. Die Objektklasse wird als Eintragsattribut gespeichert und bestimmt, welche Attribute in einem Eintrag erforderlich und zulässig sind. Häufig verwendete Objektklassenwerte sind "person", "organizationalUnit" und "organizationalPerson". Mit Objektklassenkombinationen lassen sich komplexe Einträge darstellen, wie zum Beispiel die Angestellten einer Firma.

Verzeichnisdienste und pcAnywhere

In den Verzeichnisdiensten wird der Host gestartet und wartet wie gewohnt auf ankommende Anrufe. Gleichzeitig stellt der Host eine Verbindung zu einem LDAP-Server her und aktualisiert den Benutzereintrag durch Hinzufügen eines Attributs, das die aktuelle IP-Adresse, den Computernamen und den aktuellen Status des Hosts speichert.

Beim Starten des Remote-Rechners wird eine neue Anwendung, der Verzeichnisdienst-Browser, ausgeführt und stellt die Verbindung zu einem LDAP-Server her. Der Verzeichnisdienst-Browser ruft alle Einträge ab, die seine Filterkriterien erfüllen und zeigt die Einträge in einer Liste an. Wenn Sie auf einen dieser Einträge doppelklicken, stellt der Remote die Verbindung zum ausgewählten Host her.

Konfigurieren der Verzeichnisserver

Damit Sie in pcAnywhere Verzeichnisdienste verwenden können, müssen Sie zunächst einen Verzeichnisserver für die Zusammenarbeit mit pcAnywhere konfigurieren. Folgen Sie den Anweisungen für den von Ihnen eingesetzten Verzeichnisserver.

LDAP-Server konfigurieren

Um die Verzeichnisdienste zu verwenden, fügen Sie der Konfiguration des LDAP-Servers eine benutzerdefinierte Objektklassenbeschreibung hinzu. Diese benutzerdefinierte Objektklasse beschreibt die Informationen, die der LDAP-Server für jeden Host, den ein Benutzer startet, speichern muss. Wenn die benutzerdefinierte Objektklasse vorhanden ist, können Sie alle vorhandenen Einträge bearbeiten, um Werte für die neue Objektklasse zu speichern.

Die benutzerdefinierte pcAnywhere-Objektklasse muss als "pcaHost" bezeichnet werden und darf nur ein binäres "pcaHostEntry"-Attribut enthalten:

objectclass: pcaHost

pcaHostEntry: binary

Netscape Directory Server 3.1 konfigurieren

Dazu sind Administratorrechte erforderlich.

So konfigurieren Sie Netscape Directory Server 3.1:

1. Greifen Sie mit Netscape Communicator 4.5 auf die Seite "Server Administration" zu.
2. Klicken Sie auf die Schaltfläche für den konfigurierten Verzeichnisserver.
3. Klicken Sie in der Auswahlleiste oben auf "Schema".
4. Klicken Sie in der Auswahlleiste links auf "Edit or View Attributes".
5. Geben Sie in das Feld "Attribute Name" den Eintrag "pcaHostEntry" ein.
6. Klicken Sie im Syntaxfeld auf "Binary".
7. Klicken Sie unter "Manage Attributes" auf "Add New Attribute".
8. Geben Sie das Kennwort für den Directory Manager ein, und klicken Sie dann auf "Submit".
9. Klicken Sie in der linken Auswahlleiste auf "Create Objectclass".
10. Geben Sie in das Feld "ObjectClass Name" den Eintrag "pcaHost" ein.
11. Suchen Sie in der Liste "Available Attributes" das objectclass-Attribut, und klicken Sie auf "Add", um es in die Liste "Required Attributes" aufzunehmen.
12. Suchen Sie in der Liste "Available Attributes" das pcaHostEntry-Attribut, und fügen Sie es der Liste "Allowed Attributes" hinzu.
13. Klicken Sie auf "Create New ObjectClass".
14. Geben Sie das Kennwort für "Directory Manager" ein.
15. Klicken Sie auf "Submit".
16. Starten Sie den Server neu, damit die neuen Einstellungen wirksam werden.

Netscape Directory Server 4.0 konfigurieren

Dazu sind Administratorrechte erforderlich.

So konfigurieren Sie Netscape Directory Server 4.0:

1. Starten Sie die Anwendung Netscape Console 4.0.
2. Öffnen Sie in der Strukturansicht links das Objekt, das diesen Server repräsentiert.
3. Öffnen Sie die Server-Gruppe.
4. Doppelklicken Sie auf das Objekt "Directory Server".
5. Öffnen Sie auf der Registerkarte "Configuration" in der Strukturansicht links das Objekt "Database".
6. Klicken Sie auf das Unterobjekt "Schema".
7. Klicken Sie auf der Registerkarte "Attributes" auf "Create".
8. Geben Sie in das Feld "Attribute Name" den Eintrag "pcaHostEntry" ein.
9. Klicken Sie für die Syntax auf "Binary".
10. Klicken Sie auf "Multi-Valued" und dann auf "OK".
11. Klicken Sie auf der Registerkarte "Object Classes" auf "Create".
12. Geben Sie in das Feld "Name" den Eintrag "pcaHost" ein.
13. Klicken Sie im Feld "Available Attributes" auf "objectclass".
14. Klicken Sie auf "Add", um das Feld "Required Attributes" einzuschließen.
15. Klicken Sie im Feld "Available Attributes" auf "pcaHostEntry".
16. Klicken Sie auf "Add", um das Feld "Allowed Attributes" einzuschließen.
17. Klicken Sie auf "OK", um die Objektklasse hinzuzufügen.
18. Klicken Sie auf der Registerkarte "Tasks" auf "Restart the Directory Server".
19. Klicken Sie an der Eingabeaufforderung auf "Yes".

Novell 5.0-Server konfigurieren

Die folgenden Schritte treffen nur zu, wenn LDAP auf einem Novell-Server mit Novell Directory Services (NDS) 8.0 installiert, konfiguriert und funktionsfähig ist.

Für die folgenden Schritte sind Administratorrechte für den Server erforderlich:

- pcaHostEntry konfigurieren
- pcaHost-Objekt konfigurieren
- LDAP-Attribut zuordnen
- NDS-Klasse zuordnen
- LDIF-Datei erstellen
- Rechte zuweisen

pcaHostEntry-Objekt in ConsoleOne erstellen

Führen Sie die nachfolgenden Schritte aus, um das pcaHostEntry-Objekt zu erstellen.

So erstellen Sie das pcaHostEntry-Objekt in ConsoleOne:

1. Melden Sie sich beim LDAP-Server an, auf dem sich das LDAP-Gruppenobjekt befindet.
2. Öffnen Sie ConsoleOne in sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe
3. Klicken Sie im Menü "Tools" auf "Schema Manager".
4. Klicken Sie auf der Registerkarte "Attribute" auf "Create".
5. Klicken Sie auf "Next".
6. Geben Sie in das Feld "Attribute Name" "pcaHostEntry" ein, und lassen Sie das Feld "ASNI ID" leer.

   Bei allen Eingaben wird zwischen Groß- und Kleinschreibung unterschieden.
7. Klicken Sie auf "Next".
8. Klicken Sie für die Attributsyntax auf "Octet String".
9. Klicken Sie für das Attributflag auf "Public Read".
10. Klicken Sie auf "Next".
11. Klicken Sie auf "Finish".

pcaHost-Objekt in ConsoleOne erstellen

Führen Sie die nachfolgenden Schritte aus, um das pcaHost-Objekt zu erstellen.

So erstellen Sie das pcaHost-Objekt in ConsoleOne:

1. Öffnen Sie ConsoleOne in "sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe".
2. Klicken Sie im Menü "Tools" auf "Schema Manager".
3. Klicken Sie auf der Registerkarte "Class" auf "Create".
4. Klicken Sie auf "Next".
5. Geben Sie in das Feld "Name" den Eintrag "pcaHostEntry" ein, und lassen Sie das Feld "ASNI ID" leer.

   Bei diesem Eintrag wird zwischen Groß- und Kleinschreibung unterschieden.
6. Klicken Sie auf "Next".
7. Klicken Sie auf "Auxiliary Class".
8. Klicken Sie auf "Next".
9. Doppelklicken Sie auf "Top", und fügen Sie den Eintrag dem Feld "Inherit From" hinzu.
10. Klicken Sie auf "Next".

    "Objectclass" wird im Fenster "Add these attributes" angezeigt.
11. Klicken Sie auf "Next".
12. Doppelklicken Sie auf den Eintrag "pcaHostEntry", und fügen Sie ihn zum Fenster "Add these Attributes" hinzu.
13. Klicken Sie auf "Next".

    Überprüfen Sie die Angaben für die zu erstellende neue Klasse.
14. Klicken Sie auf "Finish".

LDAP-Attribut dem NDS-Attribut zuordnen

Führen Sie die nachfolgenden Schritte aus, um das LDAP-Attribut dem NDS-Attribut zuzuordnen.

So ordnen Sie das LDAP-Attribut dem NDS-Attribut zu:

1. Doppelklicken Sie auf das Symbol für die LDAP-Gruppe.
2. Klicken Sie auf der Registerkarte "Attribute Map" auf "Add".
3. Geben Sie in das LDAP-Attributfeld "pcaHostEntry;binary" ein.
4. Klicken Sie im NDS-Attributfeld auf "pcaHostEntry".
5. Klicken Sie auf "OK".
6. Klicken Sie auf "Add".
7. Geben Sie in das LDAP-Attributfeld "pcaHostEntry" ein.
   Bei diesem Eintrag wird nach Groß- und Kleinschreibung unterschieden. Geben Sie ihn daher wie oben angegeben ein.
8. Klicken Sie im NDS-Attributfeld auf "pcaHostEntry".
9. Klicken Sie auf "OK".
10. Führen Sie eine der folgenden Aktionen aus:
    - Klicken Sie auf "Apply", um weitere Attribute zuzuordnen.
    - Klicken Sie auf "OK", um den Vorgang abzuschließen.
11. Um die Attribute für diese Zuordnung zu bearbeiten, markieren Sie das Attribut, und klicken Sie auf "Modify".

NDS-Klasse der LDAP-Klasse zuordnen

Führen Sie die nachfolgenden Schritte aus, um die NDS-Klasse der LDAP-Klasse zuzuordnen.

So ordnen Sie die NDS-Klasse der LDAP-Klasse zu:

1. Doppelklicken Sie auf das Symbol für die LDAP-Gruppe.
2. Klicken Sie auf der Registerkarte "Class Map" auf "Add".
3. Geben Sie in das LDAP-Klassenfeld "pcaHost" ein.
   Bei diesem Eintrag wird nach Groß- und Kleinschreibung unterschieden. Geben Sie ihn daher wie oben angegeben ein.
4. Klicken Sie im NDS-Attributfeld auf "pcaHost".
5. Klicken Sie auf "OK".
6. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf "Apply", um weitere Attribute zuzuordnen.
   - Klicken Sie auf "OK", um den Vorgang abzuschließen.

LDIF-Datei erstellen

Führen Sie die nachfolgenden Schritte aus, um eine LDIF-Datei zu erstellen.

Hinweis: Für diese Schritte benötigen Sie ein Textverarbeitungsprogramm wie beispielsweise Notepad sowie Zugriff auf den Server oder die Fernsteuerung über RCONAG6.NLM und RCONJ.EXE.

So erstellen Sie eine LDIF-Datei:

1. Geben Sie für jeden Benutzer die folgenden vier Zeilen in Notepad ein:
   DN:cn=user,ou=organization_unit,o=organization
   Changetype:modify
   Add:objectclass
   Objectclass:pcaHost
2. Speichern Sie diese Datei lokal, und kopieren Sie sie nach sys:system\schema\
3. Geben Sie an der Serveraufforderung **Load Bulkload.nlm** ein.
4. Klicken Sie auf "Apply LDIF file".
5. Geben Sie an der Eingabeaufforderung den Logpfad ein.
   sys:system\schema\.

Einem einzelnen Benutzer Rechte zuweisen

Führen Sie die nachfolgenden Schritte aus, um einem einzelnen Benutzer Rechte zuzuweisen.

So weisen Sie einem einzelnen Benutzer Rechte zu:

1. Wählen Sie den LDAP-Server.
2. Klicken Sie mit der rechten Maustaste auf einen Benutzer und dann auf "Trustees of the object".
3. Klicken Sie auf den Benutzer
4. Klicken Sie auf "Assigned Rights".
5. Klicken Sie auf "Add a Property".
6. Deaktivieren Sie das Kontrollkästchen "Show Only Properties of this Object Class".
7. Klicken Sie auf "pcaHostEntry".
8. Klicken Sie auf "OK".
9. Wählen Sie die Schreibzugriffsrechte, die dieser Eigenschaft hinzugefügt werden sollen.
10. Klicken Sie auf "OK".

Mehreren Benutzern Rechte zuweisen

Führen Sie die nachfolgenden Schritte aus, um mehreren Benutzern Rechte zuzuweisen.

So weisen Sie mehreren Benutzern Rechte zu:

1. Klicken Sie auf den Container, in dem die Gruppe abgelegt werden soll.
2. Klicken Sie mit der rechten Maustaste auf den Container, und klicken Sie auf "New > Group".
3. Geben Sie einen Namen für die Gruppe ein.
4. Klicken Sie mit der rechten Maustaste auf den Namen der Gruppe, und klicken Sie auf "Properties".
5. Klicken Sie auf der Registerkarte "Members" auf "Add", um andere Benutzer aufzunehmen.
6. Klicken Sie im Menü "File" auf "Properties Of Multiple Objects", um die Zugriffsrechte einzurichten.

7. Klicken Sie auf der Registerkarte "NDS Rights" auf "Add Trustee".
8. Klicken Sie auf die pcAnywhere-Gruppe, und klicken Sie dann auf "OK".
9. Klicken Sie auf "Add Property".
10. Deaktivieren Sie das Kontrollkästchen "Show Only Properties of this Object Class".
11. Klicken Sie auf "pcaHostEntry".
12. Klicken Sie auf "OK".
13. Wählen Sie die Schreibzugriffsrechte, die dieser Benutzergruppe hinzugefügt werden sollen.
14. Klicken Sie auf "OK".

Windows Active Directory konfigurieren

Der Windows 2000-Server mit Active Directory muss installiert und konfiguriert werden, bevor Sie pcAnywhere für Windows 2000 Active Directory konfigurieren.

Um Windows Active Directory mit pcAnywhere zu integrieren, müssen Sie das Schema auf dem Server erweitern. Für diesen Vorgang müssen folgenden Aufgaben ausgeführt werden:

- Snap-In hinzufügen
- pcaHostEntry-Attribut erstellen
- pcaHost-Objekt erstellen
- pcaHost-Objekt verknüpfen
- Benutzerrechte konfigurieren

Für die folgenden Schritte sind Administratorrechte für den Server erforderlich.

Snap-In hinzufügen

Führen Sie die nachfolgenden Schritte aus, um das Snap-In zur Microsoft Management Console (MMC) hinzuzufügen.

So fügen Sie das Snap-In hinzu:

1. Klicken Sie in der Windows-Taskleiste auf "Start > Ausführen".
2. Geben Sie "mmc" ein.
3. Klicken Sie auf "OK".
4. Klicken Sie auf der Symbolleiste "Console" auf "Konsole > Snap-In hinzufügen/entfernen".
5. Klicken Sie im Dialogfeld "Snap-In hinzufügen/entfernen" auf "Hinzufügen".
6. Klicken Sie auf "Active Directory-Schema" und dann auf "Hinzufügen".
7. Schließen Sie das Dialogfeld "Eigenständiges Snap-In hinzufügen".
8. Klicken Sie im Dialogfeld "Snap-In hinzufügen/entfernen" auf "OK".
9. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory-Schema", und klicken Sie dann auf "Betriebsmaster".
10. Aktivieren Sie das Kontrollkästchen "Schema kann auf diesem Domänencontroller geändert werden".
11. Klicken Sie auf "OK".

pcaHostEntry-Attribut erstellen

Führen Sie die nachfolgenden Schritte aus, um das pcaHostEntry-Attribut zu erstellen.

So erstellen Sie das Attribut "pcaHostEntry":

1. Erweitern Sie das Active Directory-Schema im linken Fensterbereich.
   Die untergeordneten Ordner "Klassen" und "Attribute" sollten jetzt verfügbar sein.
2. Klicken Sie mit der rechten Maustaste auf den Ordner "Attribute", und klicken Sie dann auf "Attribut erstellen".
   Setzen Sie den Vorgang über die angezeigte Warnmeldung hinaus fort.
3. Geben Sie "pcaHostEntry" in das Feld "Gemeinsamer Name" ein.
   Bei diesem Eintrag wird nach Groß- und Kleinschreibung unterschieden. Geben Sie ihn daher genau wie oben angegeben ein.

4 Geben Sie in das Feld "LDAP-Anzeigename" die Zeichenfolge "pcaHostEntry" exakt wie angezeigt ein.

5 Geben Sie in das Feld "Eindeutige X500-OID" Folgendes ein:
1.3.6.1.4.1.393.100.9.8.1

6 Klicken Sie in der Syntaxliste auf "Oktett".

7 Aktivieren Sie das Kontrollkästchen "Mehrwertig".

8 Klicken Sie auf "OK".

9 Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Ordner "Klassen", und klicken Sie dann auf "Klasse erstellen".
Setzen Sie den Vorgang über die angezeigte Warnmeldung hinaus fort.

pcaHost-Objekt erstellen

Führen Sie die nachfolgenden Schritte aus, um das pcaHost-Objekt zu erstellen.

So erstellen Sie das pcaHost-Objekt:

1 Geben Sie "pcaHost" in das Feld "Gemeinsamer Name" ein.
Bei diesem Eintrag wird nach Groß- und Kleinschreibung unterschieden. Geben Sie ihn daher genau wie oben angegeben ein.

2 Geben Sie in das Feld "LDAP-Anzeigename" die Zeichenfolge "pcaHost" exakt wie angezeigt ein.

3 Geben Sie in das Feld "Eindeutige X500-OID" Folgendes ein:
1.3.6.1.4.1.393.100.9.8.2

4 Geben Sie **Top** in das Feld "Übergeordnete Klasse" ein.

5 Klicken Sie in der Liste "Klasse" auf "Zusätzlich".

6 Klicken Sie auf "Weiter".

7 Klicken Sie im Dialogfeld "Neue Schemaklasse erstellen" auf die Schaltfläche "Hinzufügen" für das Feld "Optionales Attribut".

8 Wählen Sie das pcaHostEntry-Attribut.

9 Klicken Sie auf "OK".
Das Attribut pcaHostEntry sollte als optionales Attribut angezeigt werden.

10 Klicken Sie auf "Fertig stellen".

pcaHost-Objekt mit der Benutzerobjektklasse verknüpfen

Führen Sie die nachfolgenden Schritte aus, um das pcaHost-Objekt mit der Benutzerobjektklasse zu verknüpfen.

So verknüpfen Sie das pcaHost-Objekt mit der Benutzerobjektklasse:

1. Erweitern Sie im linken Fensterbereich der Console1 den Ordner "Klasse".
2. Klicken Sie mit der rechten Maustaste auf die Benutzerobjektklasse, und klicken Sie auf "Eigenschaften".
3. Klicken Sie auf die Registerkarte "Beziehung", und klicken Sie auf "Hinzufügen" für das Feld "Erweiterungsklassen".
4. Wählen Sie die pcaHost-Objektklasse.
5. Klicken Sie auf "OK".
6. Klicken Sie auf "Übernehmen".
7. Klicken Sie auf "OK".
8. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory-Schema".
9. Klicken Sie auf "Schema neu laden".

Rechte für den pcAnywhere-Benutzer konfigurieren

Um die Rechte für den pcAnywhere-Benutzer einzurichten, müssen Sie zuerst Anzeigerechte und dann Bearbeitungsrechte konfigurieren.

So konfigurieren Sie Anzeigerechte für den Benutzer:

1. Klicken Sie in der Windows-Taskleiste auf "Start > Programme > Verwaltung > Active Directory-Benutzer und -Computer".
2. Stellen Sie sicher, dass im Menü "Ansicht" die Option "Erweiterte Funktionen" aktiviert ist.

   Hiermit wird die Registerkarte "Sicherheit" auf den Eigenschaftenseiten aktiviert.

   Sie können die folgenden Rechte für jede Organisationseinheit konfigurieren. Im Idealfall sollten Sie diese Rechte auf der Ebene konfigurieren, auf der die pcAnywhere-Benutzer installiert sind.
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, und klicken Sie dann auf "Eigenschaften".
4. Klicken Sie auf der Registerkarte "Sicherheit" auf "Hinzufügen".

5. Klicken Sie auf die Gruppe "Jeder".
6. Klicken Sie auf "Hinzufügen".
7. Klicken Sie auf "OK".
8. Aktivieren Sie in der Spalte "Zulassen" die Option "Schreibgeschützt".
9. Klicken Sie auf der Eigenschaftenseite der Organisationseinheit auf "Erweitert".
10. Wählen Sie die Gruppe "Jeder" aus, die Sie gerade hinzugefügt haben.
11. Klicken Sie auf "Anzeigen/Bearbeiten".
12. Klicken Sie auf der Registerkarte "Objekt" in der Liste "Übernehmen für" auf "Dieses und alle untergeordneten Objekte".
13. Klicken Sie so oft auf "OK", bis die Eigenschaftenseite "Sicherheit" geschlossen wird.

Bearbeitungsrechte für den Benutzer konfigurieren

Führen Sie die nachfolgenden Schritte aus, um Bearbeitungsrechte für den Benutzer zu konfigurieren.

So konfigurieren Sie Bearbeitungsrechte für den Benutzer:

1. Klicken Sie auf der Registerkarte "Sicherheit" der Organisationseinheit auf "Hinzufügen".
2. Klicken Sie auf die Gruppe "Selbst".
3. Klicken Sie auf "Hinzufügen".
4. Klicken Sie auf "OK".
5. Aktivieren Sie in der Spalte "Zulassen" die Option "Schreiben".
6. Klicken Sie auf "Weitere".
7. Wählen Sie die Gruppe "Selbst" aus, die Sie soeben hinzugefügt haben, und klicken Sie dann auf "Anzeigen/Bearbeiten".
8. Klicken Sie auf der Registerkarte "Objekt" in der Liste "Übernehmen für" auf "Nur untergeordnete Objekte".
9. Klicken Sie so oft auf "OK", bis die Eigenschaftenseite "Sicherheit" geschlossen wird.

Konfigurieren von pcAnywhere für die Verwendung von Verzeichnisdiensten

Um pcAnywhere für die Verwendung von Verzeichnisdiensten zu konfigurieren, müssen die nachfolgenden Schritte ausgeführt werden:

- Verzeichnisdienste in den pcAnywhere-Einstellungen einrichten, so dass alle Verbindungsobjekte mit den gleichen Einstellungen arbeiten.
- Verzeichnisdienste für ein Host-Verbindungsobjekt einrichten
- Verzeichnisdienste für ein Remote-Verbindungsobjekt einrichten.

Verzeichnisdienste in pcAnywhere einrichten

Bevor Sie die nachfolgenden Schritte ausführen, müssen Sie zunächst die Verzeichnisservereinträge konfigurieren.

So richten Sie Verzeichnisdienste in pcAnywhere ein:

1. Klicken Sie in pcAnywhere-Manager im Menü "Bearbeiten" auf "Voreinstellungen".
2. Klicken Sie im pcAnywhere-Fenster "Optionen" auf der Registerkarte "Verzeichnisdienste" auf "Hinzufügen".
3. Geben Sie in das Feld "Angezeigter Name" einen Namen ein, mit dem der Verzeichnisserver deutlich beschrieben wird.
4. Geben Sie in das Feld "Verzeichnisserver" den Host-Namen oder die IP-Adresse des Verzeichnisservers ein.
5. Geben Sie in das Feld "Name" den auf dem Verzeichnisserver angegebenen Kontonamen ein.
6. Geben Sie in das Feld "Kennwort" das Kennwort ein, mit dem das Konto authentifiziert wird.

   Für das Kennwort wird zwischen Groß- und Kleinschreibung unterschieden.
7. Klicken Sie auf "Weitere Optionen", um die Anschlussnummer und die Suchbasis der Verzeichnisstruktur zu konfigurieren.

   Diese Informationen sollten Sie in jedem Fall konfigurieren.
   Die Anschlussnummer steuert den Anschluss, den der Verzeichnisserver verwendet, um Abfragen vom Client zu akzeptieren. Der Standardanschluss ist 389. Als Suchbasis wird das Stammverzeichnis der Verzeichnisstruktur verwendet, in der die Suchabfragen beginnen.

8 Klicken Sie auf "OK".

Symantec pcAnywhere versucht, eine Verbindung zum Verzeichnisserver herzustellen und nach dem im Feld "Name" angegebenen Eintrag zu suchen. Werden mehrere Einträge gefunden, muss der Benutzer den entsprechenden Eintrag auswählen. Nachdem der Eintrag identifiziert wurde, speichert pcAnywhere den definierten Namen (Distinguished Name, DN) in der Registrierung, um die Identifizierung zu erleichtern, und kennzeichnet den Eintrag als "Geprüft".

Hinweis: Häufige Gründe für ein Fehlschlagen der Überprüfung sind: die Trennung der Verbindung zum Netzwerk, falsche TCP/IP Konfigurationseinstellungen, die Verwendung eines falschen Benutzernamens bzw. Kennworts oder die fehlende Konfiguration von Benutzerinformationen auf dem Server.

Host-Computer für die Verwendung von Verzeichnisdiensten einrichten

Wenn Sie eine Host-Verbindung für die Verwendung von Verzeichnisdiensten einrichten, durchsucht pcAnywhere den Verzeichnisserver beim Start der Host-Verbindung nach dem angegebenen gemeinsamen Namen (CN, Common Name). Wird ein entsprechender Eintrag gefunden, aktualisiert pcAnywhere diesen mit den Verbindungsinformationen und dem aktuellen Host-Status.

Bei einer Änderung des Status aktualisiert der Host seinen Eintrag im Verzeichnisserver, so dass der aktuelle Status für alle Remote-Computer verfügbar ist. Wenn der Host beendet wird, wird der Eintrag des Host-Benutzers zurückgesetzt.

So richten Sie den Host-Computer für die Verwendung von Verzeichnisdiensten ein:

1. Klicken Sie in pcAnywhere-Manager auf "Hosts".
2. Klicken Sie mit der rechten Maustaste auf ein Host-Verbindungsobjekt, das mit einer Netzwerkverbindung arbeitet, und klicken Sie anschließend auf "Eigenschaften".
3. Klicken Sie auf der Registerkarte "Einstellungen" auf "Verzeichnisdienste verwenden".
4. Wählen Sie den geeigneten Verzeichnisserver aus der Liste aus.
5. Klicken Sie auf "OK".

   Mit dem im Feld "Verzeichnisserver" ausgewählten Verzeichnisservereintrag wird dieser Host beim Starten registriert.

Remote-Computer für die Verwendung von Verzeichnisdiensten einrichten

Wenn Sie eine Remote-Verbindung für die Verwendung von Verzeichnisdiensten einrichten, sucht der Remote-Computer auf dem Verzeichnisserver nach wartenden Host-Verbindungen.

So richten Sie den Remote-Computer für die Verwendung von Verzeichnisdiensten ein:

1. Klicken Sie in pcAnywhere-Manager auf "Remotes".
2. Klicken Sie mit der rechten Maustaste auf ein Remote-Verbindungsobjekt, das mit einer Netzwerkverbindung arbeitet, und klicken Sie anschließend auf "Eigenschaften".
3. Klicken Sie auf der Registerkarte "Einstellungen" auf "Verzeichnisdienste verwenden".
4. Wählen Sie einen Verzeichnisserver aus der Liste aus.

   In der Liste werden nur die vorkonfigurierten und überprüften Verzeichnisserver geführt.
5. Klicken Sie auf "Filter", um die anfänglichen Filtereinstellungen zu konfigurieren.

   Auf der Filter-Seite können Sie das Suchergebnis gezielt einschränken. Nehmen Sie in bestimmten oder allen Feldern Einträge vor. Nur die Einträge, die diese Kriterien erfüllen, werden zurückgegeben. In diesen Feldern werden Platzhalterzeichen unterstützt. Zum Beispiel gibt A* alle Einträge zurück, die mit dem Buchstaben "A" beginnen.

Kapitel 6

Sicherheit in Symantec pcAnywhere

In diesem Kapitel werden folgende Themen behandelt:

- Methoden zum Sichern von pcAnywhere
- pcAnywhere und Windows-Sicherheit
- Kontrolle des Zugriffs auf pcAnywhere-Hosts
- Sichern der Sitzungen
- Überwachen von Sitzungen
- Konfigurieren einer richtliniengestützten Verwaltung

Methoden zum Sichern von pcAnywhere

Die Netzwerksicherheit nimmt aufgrund der ständig steigenden Zahl mobiler Benutzer, die externen Zugriff auf ihre Unternehmensnetzwerke benötigen, eine überragende Stellung ein. Auch die immer komplexeren Anforderungen bei der Wartung dieser Netzwerke sowie der steigende Wert des intellektuellen Eigentums, das in der Computerinfrastruktur gespeichert ist, stellt erhöhte Ansprüche an die Sicherheit. Als Administrator müssen Sie deshalb zwischen der Notwendigkeit des Remote-Zugriffs und dem Schutz Ihrer Systeme vor unbefugtem Zugriff und Systemüberlastungen abwägen.

Symantec pcAnywhere besitzt zahlreiche integrierte Sicherheitsfunktionen, die für die Gewährleistung einer sicheren Rechnerumgebung entwickelt wurden. Viele dieser Sicherheitsfunktionen sind in die Sicherheitsfunktionen des Netzwerkbetriebssystems integriert.

Weitere Informationen zur Verwendung und Konfiguration dieser Funktionen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

pcAnywhere und Windows-Sicherheit

Symantec pcAnywhere läuft unter allen Microsoft Windows 32-Bit-Betriebssystemen. Wenn die Wahrung der höchsten Sicherheitsstufe jedoch eine Priorität ist, sind als Betriebssysteme eher Windows NT/2000/XP zu empfehlen. Diese Betriebssysteme sind auf Sicherheit ausgelegt.

Symantec pcAnywhere nutzt Sicherheitsfunktionen von Windows NT/2000/XP, wie beispielsweise Benutzerauthentifizierung, Ereignisprotokollierung und Datenverschlüsselung. Zur Gewährleistung der höchsten Sicherheitsstufe sollten Sie jedoch die vom Betriebssystem bereitgestellten Sicherheitsmaßnahmen nutzen.

Obwohl Windows NT/2000/XP zu den sichersten Betriebssystemen gehören, die der Markt zu bieten hat, wird die Sicherheit dieser Betriebssysteme durch öffentliche Interessengruppen, Hobby-Anwender sowie Benutzer und Hacker, die destruktive Absichten verfolgen, ständig auf die Probe gestellt. Administratoren wird empfohlen, sich in Newsgruppen, auf der Symantec Website und anderen bekannten Websites über das Thema Sicherheit zu informieren. Viele Websites, einschließlich symantec.com, bieten Patches an, um neu erkannten Sicherheitsrisiken zu begegnen.

Kontrolle des Zugriffs auf pcAnywhere-Hosts

Der erste Schritt zur Absicherung einer Computerumgebung besteht in der Kontrolle des Remote-Zugriffs auf das Netzwerk. Administratoren sollten die Zahl der externen Zugriffspunkte auf ihre Netzwerkinfrastruktur reduzieren. Zu diesem Zweck können Sie die Anzahl von Netzwerk-Hosts, die für den Fernzugriff verfügbar sind, reduzieren, und sichere RAS- und VPN-Lösungen anstelle von einzelnen DFÜ-Geräten installieren.

Mit den folgenden Methoden können Sie den Zugriff auf pcAnywhere-Hosts kontrollieren:

- Verbindungen nur für bestimmte Computernamen oder IP-Adressen zulassen

  Siehe "Verbindungen nur für bestimmte Computernamen oder IP-Adressen zulassen" auf Seite 140.

- pcAnywhere-Installationen eine Seriennummer zuweisen

  In Symantec pcAnywhere können Sie benutzerdefinierte Installationspakete mit einem Sicherheitscode in Form einer integrierten Seriennummer erstellen. Diese Seriennummer muss sowohl auf dem Host- als auch auf dem Remote-Computer vorhanden sein, damit eine Verbindung hergestellt werden kann.

  Siehe "pcAnywhere-Installation eine Seriennummer zuweisen" auf Seite 30.

- Authentifizierungsmethode einrichten

  Symantec pcAnywhere unterstützt eine Reihe von zentralen Authentifizierungstypen, wie z. B. Active Directory, Novell Directory Services, Novell Bindery, Windows NT und RSA SecurID. Auf diese Weise können Sie die in Ihrem Netzwerk bereits vorhandenen Authentifizierungsmethoden nutzen.

  Siehe "Zentrale Authentifizierung in pcAnywhere nutzen" auf Seite 141.

- Nach ungesicherten Hosts suchen

  Mit dem Remote Access Perimeter Scanner können Sie das Netzwerk und die Telefonleitungen nach ungeschützten Fernzugriffs-Hosts durchsuchen und Sicherheitslücken schließen. Dieses separat zu installierende Administrator-Tool finden Sie auf der Symantec pcAnywhere Corporate-CD.

  Siehe "Erkennen von Sicherheitsrisiken" auf Seite 157.

- Anmeldeversuche pro Anruf begrenzen

  Das Begrenzen der Anmeldeversuche eines Remote-Benutzers bei einem Host-Computer schützt vor Hackern und Denial-of-Service-Angriffen. Symantec pcAnywhere trennt die Verbindung, falls sich ein Remote-Benutzer vor Erreichen dieses Grenzwerts nicht anmelden kann.

  Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

- Anmeldungszeitraum begrenzen

  Das Begrenzen des Zeitraums für die Anmeldung eines Remote-Benutzers bei einem Host-Computer schützt vor Hackern und Denial-of-Service-Angriffen.

  Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

- Bestätigungsabfrage bei Verbindung

  Wenn Sie diese Option aktivieren, benachrichtigt pcAnywhere den Host-Benutzer, dass jemand versucht, eine Verbindung herzustellen. Der Host-Benutzer hat die Möglichkeit, die Verbindung zuzulassen oder zu verweigern.

  Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Verbindungen nur für bestimmte Computernamen oder IP-Adressen zulassen

Blockieren Sie externe Verbindungen zu einem pcAnywhere-Host, indem Sie den Host so konfigurieren, dass nur die Verbindungen zulässig sind, die innerhalb eines bestimmten Teilnetzes oder eines bestimmten TCP/IP-Adressbereichs liegen. Remote-Benutzer außerhalb der Firewall müssen über einen sicheren Tunnel oder ein VPN, das innerhalb des angegebenen Adressbereichs liegt, eine Verbindung herstellen.

Jeder erfahrene Hacker kann diese Maßnahme umgehen, indem er eine gültige IP-Adresse ausfindig macht. Um eine optimale Sicherheit zu gewährleisten, sollten Sie diese Funktion in Kombination mit der Zuweisung einer Seriennummer verwenden.

So lassen Sie Verbindungen nur für bestimmte Computernamen oder IP-Adressen zu:

1. Klicken Sie in pcAnywhere-Manager im Menü "Bearbeiten" auf "Voreinstellungen".
2. Geben Sie im pcAnywhere-Fenster "Optionen" auf der Registerkarte "Host-Kommunikation" unter "Verbindungen auf folgende Namen oder IP-Adressen beschränken" den Computernamen oder die IP-Adresse der Remote-Benutzer ein, für die Verbindungen zulässig sein sollen.
3. Klicken Sie auf "Beschränkung hinzufügen".
4. Wiederholen Sie die Schritte 2 und 3 für jeden Computernamen oder jede IP-Adresse, für den bzw. die Verbindungen zulässig sein sollen.
5. Klicken Sie auf "OK".

Zentrale Authentifizierung in pcAnywhere nutzen

Sie müssen in Symantec pcAnywhere für alle Remote-Benutzer oder -Benutzergruppen, die Verbindungen zu Ihrem Host-Computer herstellen, ein Anruferanmeldekonto einrichten. Ferner müssen Sie eine Authentifizierungsmethode für die Überprüfung der Identität dieser Benutzer auswählen. Um unbefugte Zugriffe zu verhindern, werden diese Informationen für alle Host-Sitzungen benötigt.

Symantec pcAnywhere unterstützt eine Reihe zentraler Authentifizierungstypen, wie z. B. Active Directory, Novell Directory Services, Novell Bindery, Windows NT und RSA SecurID. Auf diese Weise können Sie die in Ihrem Netzwerk bereits vorhandenen Authentifizierungsmethoden nutzen.

Zweifaktorenauthentifizierung

Symantec pcAnywhere unterstützt die RSA SecurID-Zweifaktorenauthentifizierung. SecurID prüft Benutzer anhand eines Sicherheitscodes, der für die Echtheitsbestätigung generiert wird, und einem vom Benutzer angegebenen PIN.

Die RSA ACE/Server und Agenten müssen im Netzwerk ordnungsgemäß installiert und konfiguriert sein.

Weitere Informationen finden Sie auf der RSA-Website unter folgender Adresse:

www.rsa.com

Führen Sie die folgenden Schritte aus, um SecurID in pcAnywhere zu implementieren:

- Installieren und konfigurieren Sie den RSA ACE/Agenten auf dem Host-Computer.
  Weitere Informationen finden Sie in der Dokumentation von RSA.
- Öffnen Sie pcAnywhere auf dem Host-Computer, und konfigurieren Sie ein Host-Verbindungsobjekt für die SecurID-Authentifizierung.
  Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Wenn ein Remote-Benutzer versucht, eine Verbindung zu einem Host-Computer herzustellen, der die SecurID-Authentifizierung verwendet, wird der Benutzer zur Eingabe von Authentifizierungs-Anmeldeinformationen aufgefordert. Hierzu zählen eine PIN-Nummer, ein Anmeldename und ein Passcode.

Der Host-Computer verarbeitet die Datenanforderungen zwischen dem Remote-Computer und dem RSA ACE/Agenten, der auf dem Host-Computer installiert ist. Der RSA ACE/Agent verarbeitet die Datenanforderungen zwischen dem Host-Computer und dem RSA ACE/Server.

Falls der vom Remote-Benutzer eingegebene Tokencode nicht mit der Serveruhrzeit übereinstimmt oder manipuliert zu sein scheint, wird der Benutzer zur Eingabe eines anderen Tokencodes aufgefordert. Dieser nächste Tokencode wird von der SecurID-Echtheitsbestätigung generiert. Erst wenn dieser Tokencode generiert wurde, kann der Remote-Benutzer fortfahren.

Hinweis: Die RSA SecurID-Authentifizierung kann allerdings nur verwendet werden, wenn sowohl auf dem Host- als auch auf dem Remote-Computer Symantec pcAnywhere 11.0 ausgeführt wird.

Microsoft Windows-basierte Authentifizierungstypen

Tabelle 6-1 enthält Informationen zu den Authentifizierungstypen, die es für Microsoft Windows-basierte Plattformen gibt.

Tabelle 6-1 Microsoft Windows-basierte Authentifizierungstypen

Microsoft Windows-basierte Authentifizierungstypen	Beschreibung	Implementierung in pcAnywhere
ADS (Active Directory Server) (nur für Windows 2000)	Führt die Überprüfung eines Benutzers oder einer Gruppe anhand einer Liste durch, die in einem Active Directory-Dienst gespeichert ist.	Benutzer können einen ADS-Baum nach Benutzer- oder Gruppennamen durchsuchen.
Microsoft LDAP	Führt die Authentifizierung anhand einer Benutzerliste durch, die im LDAP 3.0-kompatiblen (LDAP, Lightweight Directory Access Protocol) Verzeichnisdienst gespeichert ist.	Benutzer müssen sich auf dem LDAP-Server anmelden und können dann nach Benutzernamen suchen.
NT (nur für Windows NT und Windows 2000)	Überprüft einen Benutzer oder eine Gruppe anhand einer Arbeitsstations- oder Benutzer-Domänenliste.	Windows NT-Benutzer können eine Domänenliste nach Benutzer- und Gruppennamen durchsuchen.
Windows	Überprüft einen Benutzer oder eine Gruppe anhand eines im Microsoft-Netzwerk freigegebenen Verzeichnisses.	Windows 9x- oder Windows Me-Benutzer können ein freigegebenes Verzeichnis nach Benutzer- oder Gruppennamen durchsuchen.

Windows NT-Authentifizierung für globale Benutzer konfigurieren

Mit Symantec pcAnywhere können Sie einen Server mit Hilfe der Windows NT-Authentifizierung konfigurieren, um Anrufer aus der Benutzergruppe des lokalen Administrators sowie aus allen anderen globalen Gruppen, die in der lokalen Gruppe installiert sind, zu unterstützen.

Mit Hilfe dieser Funktion können Sie ein Anruferkonto auf einem Server für alle Administratoren in Ihrem Unternehmen einrichten, indem Sie ein Domänenkonto zur Gruppe der lokalen Administratoren hinzufügen. Diese Konfigurationsoption ist weniger zeitaufwendig als wenn Sie für jeden Administrator ein einzelnes Konto zur Gruppe der lokalen Administratoren hinzufügen.

Diese Funktion wird nur für die Windows NT-Authentifizierung unterstützt.

So richten Sie die Windows NT-Authentifizierung für globale Benutzer ein:

1. Klicken Sie in pcAnywhere-Manager auf der linken Navigationsleiste auf "Hosts".
2. Führen Sie eine der folgenden Aktionen aus:
   - Um ein neues Verbindungsobjekt hinzuzufügen, klicken Sie im Menü "Datei" auf "Neu > Objekt > Weitere Optionen".
   - Um ein vorhandenes Verbindungsobjekt zu ändern, klicken Sie im rechten Fensterbereich unter "Host" mit der rechten Maustaste auf ein Verbindungsobjekt, und klicken Sie dann auf "Eigenschaften".
3. Klicken Sie im Host-Eigenschaftenfenster auf der Registerkarte "Anrufer" unter "Authentifizierungstyp" auf "NT".
4. Führen Sie eine der folgenden Aktionen aus:
   - Um einen neuen Anrufer hinzuzufügen, doppelklicken Sie unter "Anruferliste" auf das Symbol "Neues Objekt".
   - Um einen vorhandenen Anrufer zu ändern, doppelklicken Sie in der Anruferliste auf einen Namen.
5. Aktivieren Sie im Fenster "Anrufereigenschaften" auf der Registerkarte "Identifikation" das Kontrollkästchen "In lokalen NT-Gruppen def. glob. NT-Benutzer/-Gruppen unterstützen".
6. Klicken Sie auf "OK".

Novell-basierte Authentifizierungstypen

Tabelle 6-2 enthält Informationen zu den Authentifizierungstypen, die es für Novell-basierte Plattformen gibt.

Hinweis: Für die Novell-basierte Authentifizierung ist Novell NetWare Client 32 erforderlich.

Tabelle 6-2 Novell-basierte Authentifizierungstypen

Novell-basierte Authentifizierungstypen	Beschreibung	Implementierung in pcAnywhere
Novell Bindery	Führt die Überprüfung anhand einer Liste durch, die in einer Novell NetWare Bindery gespeichert ist.	Benutzer müssen den Namen des Servers und einen gültigen Benutzernamen angeben.
NDS	Führt die Überprüfung eines Benutzers oder einer Gruppe anhand einer Liste durch, die in einem Novell Directory Services gespeichert ist.	Benutzer können einen NDS-Baum nach Benutzer- oder Gruppennamen durchsuchen.
Novell LDAP	Führt die Überprüfung eines Benutzers oder einer Gruppe anhand einer Liste durch, die in einem LDAP 3.0-kompatiblen Verzeichnisdienst gespeichert ist.	Benutzer müssen sich auf dem LDAP-Server anmelden und können dann nach Benutzernamen suchen.

Webbasierte Authentifizierungsmethoden

Tabelle 6-3 enthält Informationen zu den verfügbaren webbasierten Authentifizierungstypen.

Tabelle 6-3 Webbasierte Authentifizierungstypen

Webbasierte Authentifizierungs-methoden	Beschreibung	Implementierung in pcAnywhere
FTP	Ein Host, der auf einem FTP-Server ausgeführt wird, überprüft einen Benutzer anhand einer Benutzerliste, die mit dem FTP-Dienst verbunden ist. Der Benutzername und das Kennwort werden in Klartext über das Netzwerk übertragen.	Benutzer müssen einen Servernamen und einen gültigen Benutzernamen angeben.
HTTP-Anrufer-authentifizierung	Ein Host, der auf einem HTTP-Internet-Server ausgeführt wird, überprüft einen Benutzer anhand einer Benutzerliste, die mit dem HTTP-Dienst verbunden ist. Der Benutzername und das Kennwort werden in Klartext über das Netzwerk übertragen.	Benutzer müssen einen Servernamen und einen gültigen Benutzernamen angeben.
HTTPS-Anrufer-authentifizierung	Ein Host, der auf einem HTTPS-Internet-Server ausgeführt wird, überprüft einen Benutzer anhand einer Liste, die mit einem HTTPS-Dienst verbunden ist. Diese Methode ist sicherer als die FTP- und HTTP-Authentifizierung, da der Benutzername und das Kennwort vor der Übertragung über das Netzwerk verschlüsselt werden.	Benutzer müssen einen Servernamen und einen gültigen Benutzernamen angeben.
Anrufer-authentifizierung mit Netscape LDAP	Führt die Überprüfung eines Benutzers anhand einer Liste durch, die in einem LDAP 3.0-kompatiblen Verzeichnisdienst gespeichert ist.	Benutzer müssen sich auf dem LDAP-Server anmelden und können dann nach Benutzernamen suchen.

Sichern der Sitzungen

Symantec pcAnywhere bietet eine Reihe von Optionen, mit denen die Vertraulichkeit Ihrer Sitzung gesichert und die Ausführung von Aktionen, die die Host-Sitzung stören könnten, verhindert werden kann. Diese Sicherheitsmaßnahmen bieten zusätzliche Sicherheit, sind jedoch in Verbindung mit stärkeren Sicherheitsfunktionen in pcAnywhere am effektivsten. Zu diesen Maßnahmen zählen die Authentifizierung und die Verschlüsselung, wodurch der Host vor unbefugten Zugriffen und absichtlichen Dienstunterbrechungen geschützt wird.

pcAnywhere bietet unter anderem die folgenden Methoden, um Sitzungen zu schützen:

- Starke Verschlüsselung

  Schützen Sie den Datenstrom einschließlich des Autorisierungsvorgangs mit Hilfe der starken Verschlüsselung vor Abhör- und Hacker-Angriffen. Symantec pcAnywhere unterstützt die starke Verschlüsselung mit öffentlichen und symmetrischen Schlüsseln. Um die Sicherheit weiter zu optimieren, können Sie mit pcAnywhere Verbindungen zu oder von einem Computer mit einer niedrigeren Verschlüsselungsstufe verweigern.

- Zeitüberschreitungswerte bei Inaktivität für Sitzungen

  Schützen Sie den Host vor Benutzern, die versehentlich vergessen, eine Sitzung zu beenden. Die Verbindung zum Host wird getrennt, wenn während eines bestimmten Zeitraums keine Eingabe per Tastatur oder Maus erfolgt.

- Einzelne Anruferrechte

  Mit Hilfe von Anruferrechten können Sie angeben, mit welchen Zugriffsrechten ein Remote-Benutzer auf den Host-Computer zugreifen kann. Sie können mit pcAnywhere Benutzer an der Ausführung bestimmter Funktionen auf dem Host hindern, wie zum Beispiel dem Neustarten des Host-Computers, Übertragen von Dateien zu oder vom Host-Computer oder Beenden des Hosts.

- Zeitbeschränkungen für einzelne Benutzer oder Benutzergruppen

  Schützen Sie den Host vor Benutzern mit destruktiven Absichten, die den Dienst unterbrechen möchten, sowie vor Benutzern, die versehentlich vergessen, eine Sitzung zu beenden. Legen Sie zu diesem Zweck Zeitbeschränkungen für Sitzungen fest, und konfigurieren Sie den Host so, dass die Sitzung nach einem bestimmten Zeitraum der Inaktivität automatisch beendet wird. Diese Optionen werden auf der Anruferebene konfiguriert.

- Optionen zum sicheren Beenden von Sitzungen
  Beenden Sie Host-Sitzungen auf sichere Weise, um möglichen Sicherheitsverstößen vorzubeugen. Für normal beendete Sitzungen und unvorhergesehene Sitzungsabbrüche können jeweils unterschiedliche Einstellungen vorgenommen werden. Zu den Sicherheitsfunktionen gehören Abmelden des Host-Benutzers, Neustart des Host-Computers oder Sperren des Computers. Auch können Sie festlegen, ob der Host beendet wird oder weiter auf neue Verbindungen warten soll.

Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Überwachen von Sitzungen

Mit der Ereignisprotokollierung in Symantec pcAnywhere können Sie Sitzungsaktivitäten überwachen und Informationen zu Überwachungszwecken aufzeichnen. Sie können Folgendes aufzeichnen: wer eine Verbindung zu einem Host hergestellt hat, die Sitzungsdauer, welche Dateien geöffnet wurden sowie wichtige Sicherheitsinformationen wie z. B. fehlgeschlagene Authentifizierungen oder Anmeldungen.

Je nach Betriebssystem können Sie Informationen zu Ereignissen, die während einer Sitzung stattgefunden haben, entweder an eine von pcAnywhere erstellte Logdatei, an das Windows-Ereignisprotokoll oder an ein SNMP-Protokoll (Simple Network Management Protocol) senden. Symantec pcAnywhere unterstützt die zentrale Protokollierung, und die Protokolle können auf einem sicheren, zentralen Server gespeichert werden.

Obwohl die Protokollierung ein nützliches Werkzeug ist, sollten Sie bedenken, dass sich das Aufzeichnen bestimmter Ereignisse, beispielsweise das Protokollieren jeder Datei, die auf dem Host geöffnet wird, nachteilig auf die Leistung auswirken kann. Sie sollten außerdem die Protokolldateien in bestimmten Abständen archivieren.

Weitere Informationen finden Sie im *Symantec pcAnywhere Benutzerhandbuch*.

Konfigurieren einer richtliniengestützten Verwaltung

Administratoren können die Funktionsweise von pcAnywhere mit Hilfe einer zentralen, richtliniengestützten Verwaltung anpassen. Symantec pcAnywhere unterstützt Gruppenrichtlinien in Windows 2000/XP und die Integration von Betriebssystem-Richtlinien in Windows 98/Me/NT4.

Zum Ändern von Richtlinieneinstellungen in Windows NT4/2000/XP sind Administratorrechte erforderlich.

Gruppenrichtlinien in Windows 2000/XP konfigurieren

Gruppenrichtlinien in Windows 2000/XP müssen mit dem Gruppenrichtlinien-Snap-In von Microsoft Management Console (MMC) verwaltet werden. Um Richtlinien für eine Site, Domäne oder Organisationseinheit zu verwalten, sollten Sie das Gruppenrichtlinien-Snap-In in Active Directory öffnen und dann das Gruppenrichtlinienobjekt mit dem entsprechenden Active Directory-Container verknüpfen. Das Betriebssystem enthält einen Software-Assistenten, der Sie durch diesen Vorgang führt.

Weitere Informationen zum Hinzufügen des Gruppenrichtlinien-Snap-Ins zu MMC finden Sie in der Online-Dokumentation Ihres Betriebssystems.

Symantec pcAnywhere definiert Richtlinieneinstellungen in einer Verwaltungsvorlage. Nachdem Sie das Gruppenrichtlinien-Snap-In zu MMC hinzugefügt haben, müssen Sie die Datei "pcAnywhere.adm" in MMC importieren.

Siehe "pcAnywhere-Verwaltungsvorlagen importieren" auf Seite 150.

Systemrichtlinien in Windows 98/Me/NT4 konfigurieren

Mit dem Systemrichtlinien-Editor in Windows 98/Me/NT4 können Sie Richtlinieneinstellungen unter diesen Betriebssystemen verwalten. Richtlinieneinstellungen in Windows 98/Me können von jedem Benutzer geändert werden und sind nicht so sicher wie Gruppenrichtlinien in Windows 2000/XP.

Weitere Informationen zum Systemrichtlinien-Editor finden Sie in der Online-Dokumentation Ihres Betriebssystems.

Symantec pcAnywhere definiert Richtlinieneinstellungen in einer Verwaltungsvorlage. Nachdem Sie den Systemrichtlinien-Editor gestartet haben, können Sie die Datei "pcAnywhere.adm" importieren.

Siehe "pcAnywhere-Verwaltungsvorlagen importieren" auf Seite 150.

pcAnywhere-Verwaltungsvorlagen importieren

Symantec pcAnywhere enthält Verwaltungsvorlagen zur registrierungsbasierten Richtlinienverwaltung für Windows 2000/XP und Windows 98/Me/NT4. Die pcAnywhere.adm-Dateien definieren die Richtlinieneinstellungen für bestimmte Komponenten in pcAnywhere und enthalten Registrierungsschlüssel und Werte, den Speicherort für die Registrierungseinstellungen sowie sonstige beschreibende Informationen.

pcAnywhere.adm-Datei für Windows 2000/XP importieren

Die Datei "pcAnywhere.adm" für Windows 2000/XP ist auf der pcAnywhere-CD im Ordner "Tools\Policy" gespeichert. Sie können diese Datei an einen sicheren Speicherort kopieren und dann in MMC importieren. Vor dem Importieren dieser Datei müssen Sie unbedingt das Gruppenrichtlinien-Snap-In zu MMC hinzugefügt haben.

So importieren Sie die pcAnywhere.adm-Datei für Windows 2000/XP:

1. Klicken Sie zum Starten von MMC in der Windows-Taskleiste auf "Start > Ausführen", und geben Sie **mmc** ein.
2. Wählen Sie im Konsolenfenster im linken Fensterbereich das Gruppenrichtlinienobjekt aus, für das Sie Richtlinien festlegen möchten.
3. Klicken Sie unter dem Gruppenrichtlinienobjekt mit der rechten Maustaste auf "Administrative Vorlagen", und klicken Sie dann auf "Vorlagen hinzufügen/entfernen".
4. Klicken Sie im Fenster "Vorlagen hinzufügen/entfernen" auf "Hinzufügen".
5. Wechseln Sie zum Speicherort der Datei "pcAnywhere.adm", markieren Sie sie, und klicken Sie dann auf "Öffnen".
6. Klicken Sie im Fenster "Vorlagen hinzufügen/entfernen" auf "Schließen".

pcAnywhere.adm-Datei für Windows 98/Me/NT4 importieren

Die Datei "pcAnywhere.adm" für Windows 98/Me/NT ist auf der pcAnywhere-CD im Ordner "Tools\Policy\NT4_9x_Me" gespeichert. Sie können diese Datei an einen sicheren Speicherort kopieren und dann in den Systemrichtlinien-Editor importieren. Sie müssen unbedingt die richtige pcAnywhere.adm-Datei auswählen.

So importieren Sie die pcAnywhere.adm-Datei für Windows 98/Me/NT4:

1. Klicken Sie zum Starten des Systemrichtlinien-Editors in der Windows-Taskleiste auf "Start > Ausführen", und geben Sie **poledit.exe** ein.
2. Klicken Sie im Fenster "Systemrichtlinien-Editor" im Menü "Optionen" auf "Richtlinienvorlage".
3. Klicken Sie im Fenster "Optionen für Richtlinienvorlagen" auf "Hinzufügen".
4. Wechseln Sie zum Speicherort der Datei "pcAnywhere.adm", markieren Sie sie, und klicken Sie dann auf "Öffnen".
5. Klicken Sie im Fenster "Optionen für Richtlinienvorlagen" auf "OK".

Weitere Informationen zum Ausführen des Systemrichtlinien-Editors und zum Importieren von Verwaltungsvorlagendateien finden Sie in der Online-Dokumentation Ihres Betriebssystems.

Benutzerrichtlinien verwalten

Mit Symantec pcAnywhere können Sie steuern, ob Benutzer Zugriff auf bestimmte Bereiche der Benutzeroberfläche haben oder bestimmte Funktionen in pcAnywhere ausführen können. Tabelle 6-4 enthält Informationen zu den Richtlinieneinstellungen, die Sie mit pcAnywhere steuern können.

Tabelle 6-4 Speicherort der pcAnywhere-Richtlinieneinstellungen

Ordner	Beschreibung
Actions	Enthält Richtlinieneinstellungen, um Benutzern Folgendes zu verweigern: ■ pcAnywhere-Manager, der das Hauptfenster von pcAnywhere darstellt, starten ■ Host-Objekte starten und auf diese Weise eine Host-Sitzung starten ■ Remote-Objekte starten und auf diese Weise eine Verbindung zu einem Host-Computer herstellen ■ Host-Computer, der ausgeführt wird, beenden ■ Tastatur oder Maus auf dem Host-Computer während einer Sitzung auf dem Host-Computer verwenden ■ LiveUpdate zum Downloaden von Produktaktualisierungen verwenden ■ Online-Registrierung des Produkts ■ Dialogsitzung starte; ■ Dateiübertragungs- und Befehlswarteschlangen-Funktionen verwenden
Actions\pcAnywhere Tools	Enthält Richtlinieneinstellungen, um Benutzern die Verwendung der folgenden Tools in pcAnywhere zu verweigern: ■ Paketverteilungs-Tool ■ Host-Administrator ■ Remote Access Perimeter Scanner ■ Dialogfeld "Aktivitätslogbuch bearbeiten"
Actions\Remote Management	Enthält Richtlinieneinstellungen, um Benutzern die Verwendung aller oder einzelner Remote-Verwaltungsfunktionen zu verweigern

Tabelle 6-4 Speicherort der pcAnywhere-Richtlinieneinstellungen

Ordner	Beschreibung
UI Changes\Host Objects	Enthält Richtlinieneinstellungen, um Benutzern Folgendes zu verweigern: ■ Host-Objekte bearbeiten ■ Host-Objekte erstellen ■ Speicherort von Host-Objekten ändern ■ Bestimmte Eigenschaftenseiten anzeigen oder bearbeiten ■ Den Host-Namen anpassen, der zur Identifikation des Host-Computers verwendet wird
UI Changes\ Remote Objects	Enthält Richtlinieneinstellungen, um Benutzern Folgendes zu verweigern: ■ Remote-Objekte bearbeiten ■ Remote-Objekte erstellen ■ Speicherort von Remote-Objekten ändern ■ Bestimmte Eigenschaftenseiten anzeigen oder bearbeiten
UI Changes\Option Sets	Enthält Richtlinieneinstellungen, um Benutzern Folgendes zu verweigern: ■ Optionsgruppenobjekte und globale pcAnywhere-Einstellungen bearbeiten ■ Optionsgruppenobjekte erstellen ■ Speicherort von Optionsgruppenobjekten ändern ■ Bestimmte Eigenschaftenseiten für Optionsgruppen und globale pcAnywhere-Einstellungen anzeigen oder bearbeiten
UI Changes\ Device Visibility	Enthält Richtlinieneinstellungen, um bestimmte Gerätetypen (z.B. Infrared, TAPI) aus der Liste der verfügbaren Verbindungstypen zu entfernen
UI Changes\Help	Ermöglicht die Verwendung eines benutzerdefinierten URL für die Service- und Unterstützungsoption im Hilfemenü

Benutzerrichtlinien in Windows 2000/XP verwalten

Zur Verwaltung von Benutzerrichtlinien in Windows 2000/XP müssen Sie MMC mit dem Gruppenrichtlinien-Snap-In ausführen. Sie müssen die entsprechende pcAnywhere-Verwaltungsvorlage importiert haben.

Siehe "pcAnywhere-Verwaltungsvorlagen importieren" auf Seite 150.

So verwalten Sie Benutzerrichtlinien in Windows 2000/XP:

1. Klicken Sie zum Starten von MMC in der Windows-Taskleiste auf "Start > Ausführen", und geben Sie **mmc** ein.
2. Klicken Sie im Konsolenfenster im linken Fensterbereich auf das Pluszeichen neben dem zu verwaltenden Gruppenrichtlinienobjekt, um die Liste zu erweitern.
3. Klicken Sie unter "Benutzerkonfiguration" auf das Pluszeichen neben "Administrative Vorlagen", um die Liste zu erweitern.
4. Klicken Sie auf das Pluszeichen neben Symantec pcAnywhere, um die Liste zu erweitern.
5. Öffnen Sie den Ordner, der die Richtlinieneinstellungen enthält, die Sie bearbeiten möchten.
   Siehe Tabelle 6-4, "Speicherort der pcAnywhere-Richtlinieneinstellungen," auf Seite 152.
6. Doppelklicken Sie im rechten Fensterbereich unter "Richtlinie" auf die Richtlinieneinstellungen, die Sie bearbeiten möchten.
7. Wählen Sie im Eigenschaftenfenster auf der Registerkarte "Richtlinie" eine der folgenden Optionen aus:
   - Aktiviert: Aktiviert die Richtlinie, so dass verhindert wird, dass Benutzer einen Task anzeigen oder ausführen.
   - Deaktiviert: Deaktivert die Richtlinie, so dass Benutzer einen Task anzeigen oder ausführen können.
8. Klicken Sie auf "OK".

Benutzerrichtlinien in Windows 98/Me/NT4 verwalten

Zum Verwalten von Benutzerrichtlinien in Windows 98/Me/NT4 müssen Sie den Systemrichtlinien-Editor ausführen. Auf Windows 98/Me/NT 4-Arbeitsstationen müssen Sie dieses Tool möglicherweise separat installieren. Um Benutzern Richtlinieneinstellungen bei der Anmeldung zuzuweisen, müssen Sie eine Verzeichnisfreigabe im Windows- oder NT-Ordner "system32\imports\scripts" mit dem Namen "Netlogon" erstellen.

Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrem Betriebssystem.

Bevor Sie die nachfolgenden Schritte ausführen, müssen Sie die entsprechende pcAnywhere-Verwaltungsvorlage importiert haben.

Siehe "pcAnywhere-Verwaltungsvorlagen importieren" auf Seite 150.

So verwalten Sie Benutzerrichtlinien in Windows 98/Me/NT4:

1. Klicken Sie zum Starten des Systemrichtlinien-Editors in der Windows-Taskleiste auf "Start > Ausführen", und geben Sie **poledit.exe** ein.
2. Klicken Sie im Fenster "Systemrichtlinien-Editor" im Menü "Datei" auf "Neue Richtlinie".
3. Doppelklicken Sie auf das Symbol für den Benutzer oder die Gruppe, für die Sie Richtlinien konfigurieren möchten.
4. Klicken Sie im Eigenschaftenfenster auf das Pluszeichen neben "Symantec pcAnywhere", um die Liste zu erweitern.
5. Klicken Sie unter "Symantec pcAnywhere" auf das Pluszeichen neben dem Richtlinientyp, den Sie bearbeiten möchten.
6. Aktivieren Sie die Richtlinieneinstellungen, die Sie einschalten möchten.
   Durch Aktivieren einer Richtlinieneinstellung wird verhindert, dass Benutzer einen Task anzeigen oder ausführen.
7. Klicken Sie auf "OK".
8. Speichern Sie die Richtliniendatei im Windows- oder NT-Ordner "system32\imports\scripts" unter dem Dateinamen "NTconfig.pol".

Kapitel 7

Erkennen von Sicherheitsrisiken

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zum Remote Access Perimeter Scanner
- Installieren des Remote Access Perimeter Scanner
- Öffnen des Remote Access Perimeter Scanner
- Einstellen von globalen Optionen
- Protokollieren von Remote Access Perimeter Scanner-Ereignissen
- Erstellen einer angepassten Prüfdatei
- Ausführen einer Remote Access Perimeter Scanner-Prüfung
- Anzeigen von Prüfergebnissen

Informationen zum Remote Access Perimeter Scanner

Ein falsch konfiguriertes Fernzugriffsprodukt, mit dem unbefugte Benutzer eine Verbindung zum Netzwerk herstellen und auf sicherheitskritische Informationen zugreifen können, kann ein schwerwiegendes Sicherheitsrisiko für ein Unternehmensnetzwerk darstellen. Der Remote Access Perimeter Scanner durchsucht Ihr Netzwerk nach Produkten für den Fernzugriff und erkennt mögliche Sicherheitsrisiken. Der Remote Access Perimeter Scanner ist nur in der Symantec pcAnywhere Corporate Edition verfügbar.

Mit dem Remote Access Perimeter Scanner können Sie folgende Aufgaben ausführen:

- ein Unternehmensnetzwerk und/oder Telefonnummern nach pcAnywhere und anderen Produkten für die Fernsteuerung und den Fernzugriff durchsuchen;
- ungeschützte pcAnywhere-Hosts automatisch herunterfahren;
- ein Protokoll der bei der Durchsuchung des Netzwerks ermittelten Informationen anzeigen.

Haftungsausschluss

Der Remote Access Perimeter Scanner wurde für die Identifizierung von Sicherheitsrisiken in Ihrem eigenen Unternehmen entwickelt. Die Verwendung des Remote Access Perimeter Scanner für illegale Zwecke stellt eine Verletzung der Remote Access Perimeter Scanner-Lizenzvereinbarung dar.

Jedes Mal, wenn Sie den Remote Access Perimeter Scanner öffnen, werden Sie zum Lesen der Lizenzvereinbarung aufgefordert.

Wenn Sie mit dem Remote Access Perimeter Scanner TCP/IP-Verbindungen prüfen, sendet das Programm die Meldung "Der Remote Access Perimeter Scanner überprüft Ihr System ab der TCP/IP-Adresse" an den Computer, zu dem Sie eine Verbindung herstellen, und identifiziert Ihre TCP/IP-Adresse, Ihren Benutzernamen und Ihren Computernamen.

Überprüfte Produkte

Der Remote Access Perimeter Scanner sucht nach den folgenden Produkten für den Fernzugriff:

- Symantec pcAnywhere

  Der Remote Access Perimeter Scanner sucht nach pcAnywhere für DOS 5.0, pcAnywhere 2.0 und pcAnywhere, Version 7.5 bis 11.0.

  Der Remote Access Perimeter Scanner kann pcAnywhere-Hosts, die keine Anmeldung erfordern, automatisch herunterfahren.

  Weitere Informationen finden Sie unter "Einstellen von globalen Optionen" auf Seite 162.
- LapLink 2000, Version 3.01
- Carbon Copy, Version 5.5
- Timbuktu Pro 32, Version 3.0
- ReachOut, Version 8.3
- NetSupport/PcDuo, Version 5.03
- NetMeeting, Version 3.01
- VNC, Version 3.3.3
- NetBus Pro, Version 2.0
- PPP Ras Server
- Windows DFÜ-Server
- Terminal Server für NT4
- Citrix Server
- X Server, Version 11

Installieren des Remote Access Perimeter Scanner

Der Remote Access Perimeter Scanner ist als benutzerdefinierte Installationsoption im Rahmen der vollständigen Produktinstallation verfügbar. Installieren Sie den Remote Access Perimeter Scanner wie im Folgenden beschrieben nach der Installation von pcAnywhere.

So installieren Sie den Remote Access Perimeter Scanner:

1. Klicken Sie in der Windows-Taskleiste auf "Start > Einstellungen > Systemsteuerung".
2. Doppelklicken Sie im Fenster der Systemsteuerung auf "Software".
3. Klicken Sie im Fenster "Software" auf "Symantec pcAnywhere".
4. Klicken Sie auf "Ändern".
5. Klicken Sie im Fenster zum Ändern oder Entfernen von Symantec pcAnywhere auf "Weiter".
6. Klicken Sie im Fenster "Programmverwaltung" auf "Ändern".
7. Klicken Sie auf "Weiter".
8. Klicken Sie im Fenster "Angepasstes Setup" unter "pcAnywhere-Tools" auf den Pfeil nach unten neben Remote Access Perimeter Scanner, und klicken Sie dann auf "Dieses Feature wird auf eine lokale Festplatte installiert".
9. Klicken Sie auf "Weiter".
10. Um das Programmsymbol zum Windows-Desktop hinzuzufügen, aktivieren Sie "Remote Access Perimeter Scanner".
11. Klicken Sie auf "Installieren".
12. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Installationsvorgang fortzusetzen. Klicken Sie nach Abschluss der Installation auf "Fertig stellen".
13. Falls für Ihren Computer die Aktualisierung von Systemdateien erforderlich ist, werden Sie aufgefordert, den Computer neu zu starten. Dies ist notwendig, um den störungsfreien Betrieb sicherzustellen.

Öffnen des Remote Access Perimeter Scanner

Bei den Anweisungen im restlichen Kapitel wird davon ausgegangen, dass Sie wissen, wie der Remote Access Perimeter Scanner geöffnet wird.

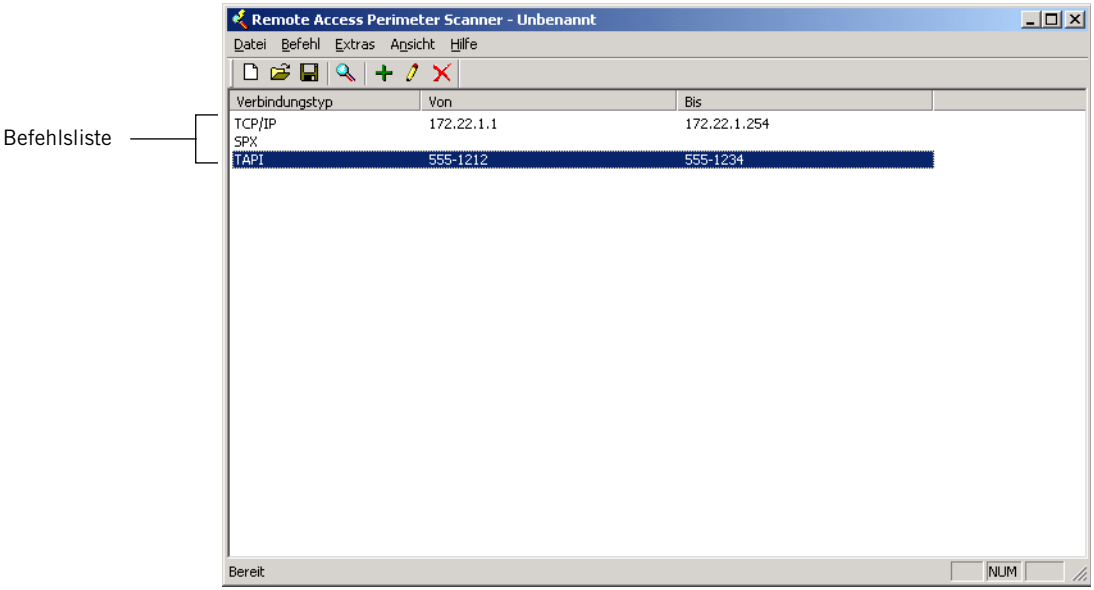
Jedes Mal, wenn Sie den Remote Access Perimeter Scanner öffnen, werden Sie aufgefordert, die Remote Access Perimeter Scanner-Lizenzvereinbarung zu lesen.

So öffnen Sie den Remote Access Perimeter Scanner:

- Klicken Sie in der Windows-Taskleiste auf "Start > Programme > Remote Access Perimeter Scanner".

  In Abbildung 7-1 wird gezeigt, wie der Inhalt einer Prüfdatei im Remote Access Perimeter Scanner-Fenster dargestellt wird.

Abbildung 7-1 Remote Access Perimeter Scanner-Prüfergebnisse



Remote Access Perimeter Scanner in der Befehlszeile ausführen

Sie können die Remote Access Perimeter Scanner-Befehlszeile verwenden, um eine Suche von einem Programmterminplaner oder einer Stapeldatei aus durchzuführen.

So führen Sie Remote Access Perimeter Scanner in der Befehlszeile aus:

- Geben Sie folgenden Befehl ein:

  raps /s dateiname.ras

  wobei /s die Prüfung startet und "dateiname.ras" dem Namen Ihrer Prüfdatei entspricht.

  Die Argumente /s und "dateiname.ras" sind optional. Wenn Sie keinen Dateinamen angeben, verwendet der Remote Access Perimeter Scanner die zuletzt von Ihnen geöffnete Prüfdatei. Wenn Sie /s nicht angeben, öffnet der Remote Access Perimeter Scanner die Prüfdatei, startet die Prüfung jedoch nicht.

  Eventuell müssen Sie auch den vollständigen Pfad zur Programmdatei des Remote Access Perimeter Scanner und den Namen der Prüfdatei eingeben.

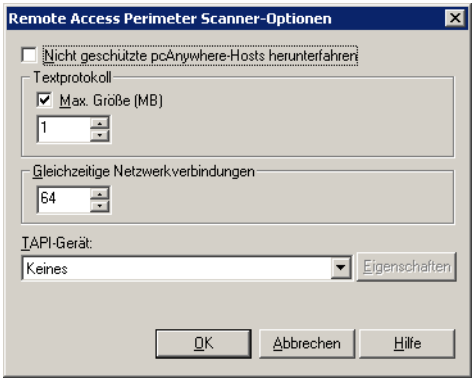
Einstellen von globalen Optionen

Darüber hinaus ist es möglich, ungesicherte pcAnywhere-Hosts automatisch herunterzufahren und Grenzwerte für die maximale Größe der vom Remote Access Perimeter Scanner erstellten Textprotokolldatei zu definieren.

Ferner können Sie auf den Umfang des Netzwerkverkehrs Einfluss nehmen, indem Sie die Anzahl simultaner Verbindungen erhöhen oder reduzieren. Des Weiteren können Sie Eigenschaften für ein TAPI-Gerät auswählen und konfigurieren.

So stellen Sie globale Optionen ein:

1 Klicken Sie im Remote Access Perimeter Scanner-Menü "Extras" auf "Optionen".



2 Aktivieren Sie im Fenster "Remote Access Perimeter Scanner-Optionen" das Kontrollkästchen "Nicht geschützte pcAnywhere-Hosts herunterfahren", wenn Sie nicht geschützte pcAnywhere-Hosts herunterfahren wollen.

3 Aktivieren Sie das Kontrollkästchen "Max. Größe (MB)", und geben Sie für das Textprotokoll die maximal zulässige Größe in Megabyte ein.

4 Legen Sie im Dialogfeld "Gleichzeitige Netzwerkverbindungen" die Netzwerknutzung fest.

Geben Sie eine niedrige Zahl ein, um den Netzwerkverkehr zu reduzieren. Verwenden Sie eine höhere Zahl, um die Geschwindigkeit der Prüfung zu erhöhen.

Diese Einstellung gilt nur für TCP/IP- und SPX-Befehle.

5 Wählen Sie in der TAPI-Geräteliste das Modem aus, das Sie für den Aufbau von TAPI-Verbindungen verwenden wollen.

6 Klicken Sie auf "OK".

Protokollieren von Remote Access Perimeter Scanner-Ereignissen

Der Remote Access Perimeter Scanner protokolliert Ereignisse separat von pcAnywhere, verwendet jedoch dieselben Methoden. Dieser Abschnitt befasst sich mit den Prozeduren für das Einrichten von SNMP-Traps, der Windows-Ereignisprotokollierung und der Protokollierung im lokalen Textprotokoll.

SNMP-Traps und die Windows-Ereignisprotokollierung sind stabiler als die einfache Text-Protokollierung. Die Textprotokollierung auf dem lokalen Computer ist während der Remote Access Perimeter Scanner-Prüfung immer aktiviert.

Ereignisprotokollklassifikationen

Der Remote Access Perimeter Scanner verwendet zwei Klassifikationen für Ereignisse: "Mögliche Schwachstelle" und "Produkt gefunden".

Wenn Remote Access Perimeter Scanner eine Verbindung mit einem Host oder Server herstellt und erkennt, dass der Host oder Server ein nicht geschütztes Fernzugriffsprodukt ausführt, protokolliert er dieses Ereignis als "Mögliche Schwachstelle".

Als weitere mögliche Schwachstellen gelten u.a. die folgenden Ereignisse:

- Der Remote Access Perimeter Scanner erkennt ein bekanntes Produkt, für das sich der Benutzer nicht anmelden muss.
- Der Remote Access Perimeter Scanner findet ein bekanntes Produkt, kann aber nicht feststellen, ob eine Benutzeranmeldung erforderlich ist.
- Der Remote Access Perimeter Scanner findet ein bekanntes Produkt, das nicht auf dem Standardanschluss ausgeführt wird.

Wenn der Remote Access Perimeter Scanner zwar eine Verbindung mit einem Host oder Server herstellen, das Produkt jedoch nicht identifizieren kann, wird dieses Ereignis als "Produkt gefunden" protokolliert.

Weitere Ereignisse, die als "Produkt gefunden" interpretiert werden:

- Der Remote Access Perimeter Scanner findet ein unbekanntes Produkt. (Unbekannt bedeutet, dass das Produkt nicht vom Remote Access Perimeter Scanner erkannt wird.)
- Der Remote Access Perimeter Scanner sucht nach einem Produkt, findet jedoch ein anderes Produkt. Beispiel: Wenn der Remote Access Perimeter Scanner nach pcAnywhere sucht und LapLink findet, dann ist LapLink bei dieser Prüfung das "unbekannte" Produkt.

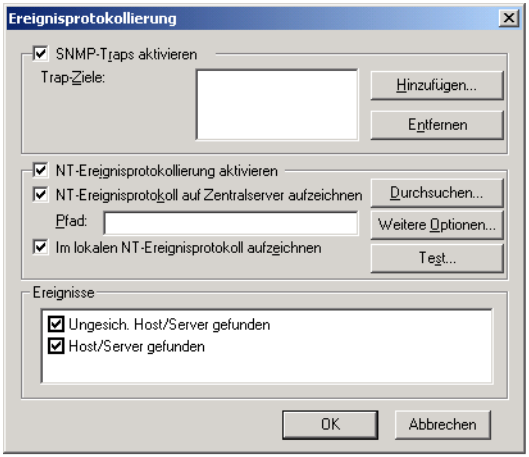
SNMP-Traps einstellen

Richten Sie SNMP-Traps wie im Folgenden beschrieben für die Protokollierung von Remote Access Perimeter Scanner-Ereignissen ein.

Siehe "Informationen zur zentralen Protokollierung" auf Seite 85.

So richten Sie SNMP-Traps ein:

1. Klicken Sie im Remote Access Perimeter Scanner-Menü "Extras" auf "SNMP und NT-Ereignisprotokollierung".
2. Aktivieren Sie im Fenster "Ereignisprotokollierung" das Kontrollkästchen "SNMP-Traps aktivieren".



3 Führen Sie einen der folgenden Schritte aus:

- Geben Sie Trap-Ziele ein, indem Sie auf "Hinzufügen" klicken.
  Im Trap-Zielfenster werden neue Trap-Ziele angezeigt.
- Klicken Sie auf "Entfernen", um ausgewählte Trap-Ziele aus der Liste zu löschen.

4 Aktivieren Sie die Ereignisse, die Sie in das Protokoll aufnehmen möchten.

5 Klicken Sie auf "OK".

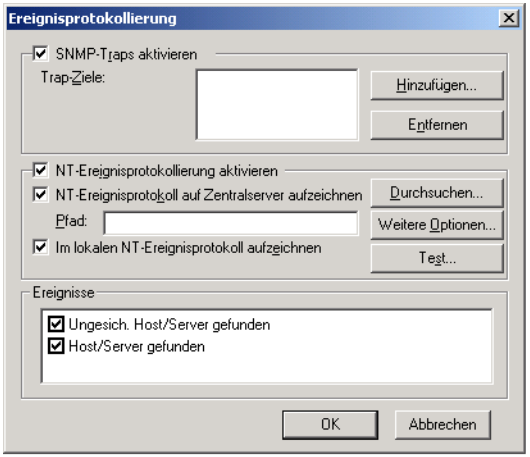
Windows-Ereignisprotokollierung einrichten

Zeichnen Sie wie im Folgenden beschrieben Remote Access Perimeter Scanner-Ereignisse im Windows-Ereignisprotokoll auf Ihrem lokalen Computer oder einem Zentralserver auf.

So richten Sie die Windows-Ereignisprotokollierung ein:

1 Klicken Sie im Remote Access Perimeter Scanner-Menü "Extras" auf "SNMP und NT-Ereignisprotokollierung".

2 Aktivieren Sie im Fenster "Ereignisprotokollierung" das Kontrollkästchen "NT-Ereignisprotokollierung aktivieren".



3 Aktivieren Sie das Kontrollkästchen "NT-Ereignisprotokoll auf Zentralserver aufzeichnen", um die Ereignisse an einem zentralen Speicherort zu speichern.

4 Geben Sie den Pfad ein, oder wechseln Sie zu dem betreffenden Pfad, indem Sie auf "Durchsuchen" klicken.

5 Klicken Sie auf "Weitere Optionen", um für den Zugriff auf den Server benötigte Authentifizierungsinformationen einzugeben.

6 Aktivieren Sie das Kontrollkästchen "Im lokalen NT-Ereignisprotokoll aufzeichnen", wenn Sie die Ereignisse lokal speichern möchten.

7 Aktivieren Sie unter "Ereignisse" die Ereignisse, die Sie in das Protokoll aufnehmen möchten.

8 Klicken Sie auf "OK".

Erstellen einer angepassten Prüfdatei

Wenn Sie sich informieren wollen, wie sicher Ihr Netzwerk ist, müssen Sie zunächst bestimmen, welche Produkte für den Fernzugriff verwendet werden. Mit dem Remote Access Perimeter Scanner können Sie feststellen, ob es in Ihrem Netzwerk Benutzer gibt, die ein nicht autorisiertes Fernzugriffsprodukt verwenden. Ferner können Sie nach ungesicherten Hosts suchen.

Damit Sie eine Remote Access Perimeter Scanner-Prüfung konfigurieren und ausführen können, müssen Sie zunächst alle Informationen sammeln, die benötigt werden, um einen Befehl zur Prüfung hinzuzufügen, beispielsweise die Telefonnummern und IP-Adressen, die durchsucht werden sollen. Anschließend können Sie eine Prüfdatei erstellen, bearbeiten und speichern.

Prüfdatei erstellen und speichern

Sie können mit dem Remote Access Perimeter Scanner mehrere Prüfdateien erstellen, um genau zu definieren, was Sie durchsuchen wollen. Oder Sie können mehrere Befehle in eine Prüfdatei einfügen. So können Sie beispielsweise mit einer Prüfdatei Ihr gesamtes Netzwerk und Telefonsystem am Wochenende durchsuchen lassen und eine weitere Prüfdatei dazu benutzen, unter der Woche die wichtigsten Netzwerkverbindungen zu überprüfen.

Nachdem Sie die Prüfdatei erstellt haben, können Sie sie durch Hinzufügen von Befehlen anpassen.

So erstellen und speichern Sie eine Prüfdatei:

1 Klicken Sie im Remote Access Perimeter Scanner-Menü "Datei" auf "Neu".

2 Wählen Sie aus, ob ein Befehl eingefügt werden soll, der im Standard-TCP/IP-Teilnetz nach pcAnywhere-Hosts sucht.

3 Klicken Sie im Remote Access Perimeter Scanner-Menü "Datei" auf "Speichern". Sie können auch **Strg**+**S** drücken.

Befehle zu einer Prüfdatei hinzufügen

Damit Sie eine Prüfung durchführen können, müssen Sie zunächst festlegen, welche Verbindungstypen Sie durchsuchen möchten. Konfigurieren Sie anschließend für jeden Verbindungstyp die Einstellungen. Mögliche Verbindungstypen sind TCP/IP, SPX, TAPI und CAPI. Für jeden Verbindungstyp muss ein separater Befehl in die Prüfdatei eingegeben werden. Es können auch mehrere Befehle für einen Verbindungstyp hinzugefügt werden. Sie können zum Beispiel mehrere TCP/IP-Befehle erstellen, mit denen unterschiedliche Teilnetze durchsucht werden.

So fügen Sie Befehle zu einer Prüfdatei hinzu:

1. Öffnen Sie die Prüfdatei, die Sie anpassen möchten, oder erstellen Sie eine neue Prüfdatei.
2. Klicken Sie im Remote Access Perimeter Scanner-Menü "Befehl" auf "Neu".
3. Wählen Sie auf der Registerkarte "Allgemein" einen Verbindungstyp aus: TCP/IP, SPX, TAPI oder CAPI.

   SPX erkennt nur pcAnywhere-Hosts.
4. Klicken Sie in der Liste "Produkte ermitteln", auf die Produkte für den Fernzugriff, nach denen Sie suchen wollen.
5. Klicken Sie auf die Registerkarte, die mit dem von Ihnen ausgewählten Verbindungstyp verknüpft ist, und führen Sie die damit verbundene Prozedur aus.

Tabelle 7-1 Remote Access Perimeter Scanner-Verbindungseinstellungen

Registerkarte	Beschreibung	Weitere Informationen finden Sie unter:
Allgemein	Wählen Sie den Verbindungstyp und die Produkte für den Fernzugriff aus, nach denen Sie suchen wollen. Diese Registerkarte wird auch beim Konfigurieren eines SPX-Befehls verwendet.	"SPX-Prüfeinstellungen konfigurieren" auf Seite 171.
TCP/IP	Geben Sie die IP-Adressen an, die Sie prüfen möchten. Sie können die IP-Adresse entweder als vollständige Teilnetzadresse oder als partielle Teilnetzadresse angeben. Darüber hinaus können Sie die Suche auf zusätzliche Anschlüsse ausdehnen.	"TCP/IP-Prüfeinstellungen konfigurieren" auf Seite 169.
TAPI	Geben Sie die Telefonnummern einschließlich Landeskennung ein, die Sie wählen wollen.	"TAPI-Prüfeinstellungen konfigurieren" auf Seite 173.
CAPI	Geben Sie die Telefonnummern ein, die Sie wählen wollen.	"CAPI-Prüfeinstellungen konfigurieren" auf Seite 174.

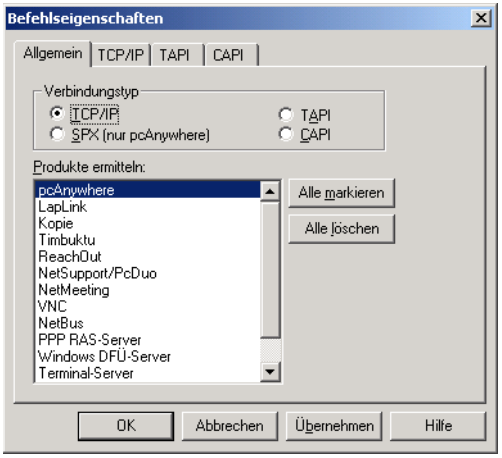
TCP/IP-Prüfeinstellungen konfigurieren

Um nach Produkten für den Fernzugriff zu suchen, die eine TCP/IP-Verbindung verwenden, müssen Sie einen TCP/IP-Befehl in Ihre Prüfdatei einfügen.

So konfigurieren Sie TCP/IP-Prüfeinstellungen:

1. Öffnen Sie die Prüfdatei, die Sie anpassen möchten, oder erstellen Sie eine neue Prüfdatei.
2. Klicken Sie im Remote Access Perimeter Scanner-Menü "Befehl" auf "Neu".

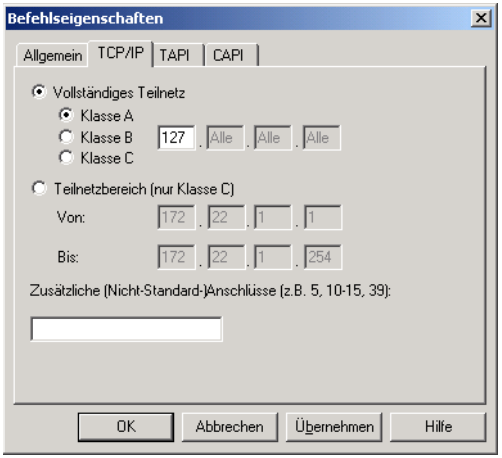
3 Klicken Sie im Befehlseigenschaftenfenster auf der Registerkarte "Allgemein" unter "Verbindungstyp" auf "TCP/IP".



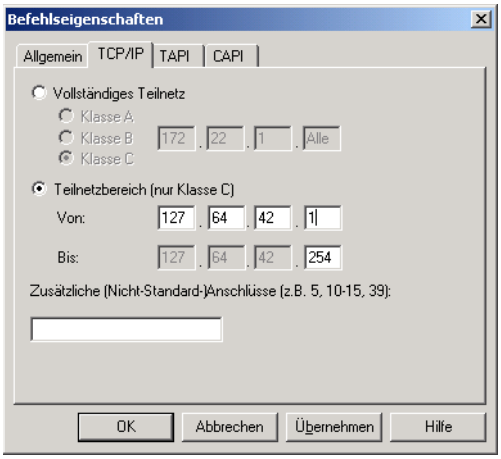
4 Wählen Sie unter "Produkte ermitteln" die Produkte aus, nach denen Sie suchen wollen.

5 Führen Sie auf der Registerkarte "TCP/IP" einen der folgenden Schritte aus:

- Klicken Sie auf "Vollständiges Teilnetz", um ein ganzes Teilnetz zu durchsuchen. Geben Sie die Adressen der Klasse A, B und C ein.



- Klicken Sie auf "Teilnetzbereich", um einen bestimmten Bereich mit Adressen der Klasse C zu durchsuchen. Geben Sie die Start- und Endadressen des Teilnetzbereichs ein.



6 Geben Sie nach Bedarf zusätzliche Anschlüsse ein, die Sie durchsuchen möchten.

7 Klicken Sie auf "OK", um den Befehl in die Prüfdatei einzufügen.

SPX-Prüfeinstellungen konfigurieren

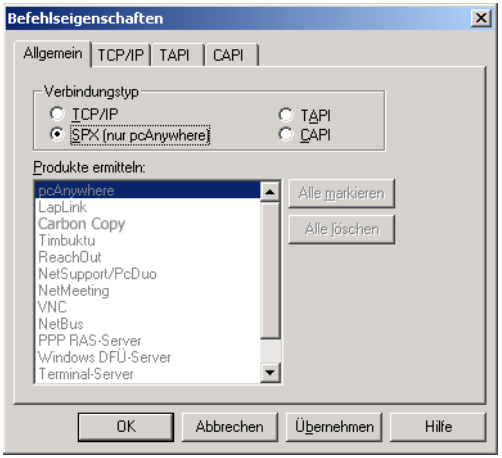
Um nach Produkten für den Fernzugriff zu suchen, die eine SPX-Verbindung verwenden, müssen Sie einen SPX-Befehl in Ihre Prüfdatei einfügen.

Bei SPX-Verbindungen sucht Remote Access Perimeter Scanner nur nach pcAnywhere.

So konfigurieren Sie SPX-Prüfeinstellungen:

1. Klicken Sie im Remote Access Perimeter Scanner-Menü "Befehl" auf "Neu".
2. Klicken Sie im Befehlseigenschaftenfenster auf der Registerkarte "Allgemein" unter "Verbindungstyp" auf "SPX (nur pcAnywhere)".

   Sobald Sie auf "SPX" klicken, wählt der Remote Access Perimeter Scanner automatisch pcAnywhere aus und deaktiviert den übrigen Teil der Liste "Produkte ermitteln".



3. Klicken Sie auf "OK", um den Befehl in die Prüfdatei einzufügen.

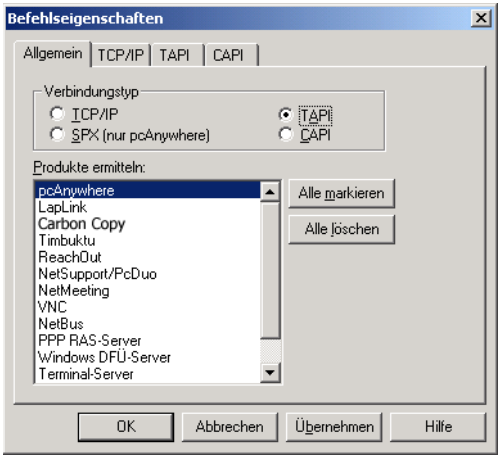
TAPI-Prüfeinstellungen konfigurieren

Um nach Produkten für den Fernzugriff zu suchen, die eine TAPI-Verbindung verwenden, müssen Sie einen TAPI-Befehl in Ihre Prüfdatei einfügen.

Symantec ist nicht für Telefongebühren verantwortlich, die möglicherweise während einer Remote Access Perimeter Scanner-Prüfung anfallen.

So konfigurieren Sie TAPI-Prüfeinstellungen:

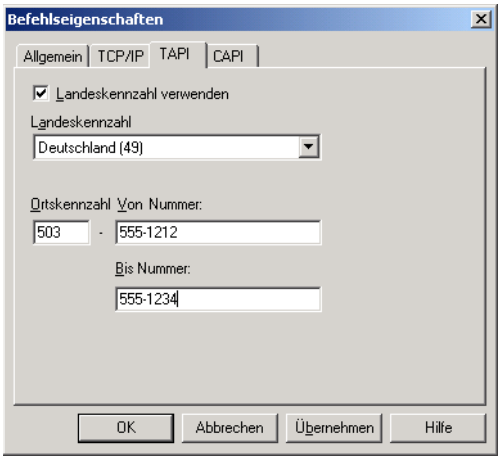
1. Öffnen Sie eine Prüfdatei, die Sie anpassen möchten, oder erstellen Sie eine neue Prüfdatei.
2. Klicken Sie im Remote Access Perimeter Scanner-Menü "Befehl" auf "Neu".
3. Klicken Sie im Befehlseigenschaftenfenster auf der Registerkarte "Allgemein" unter "Verbindungstyp" auf "TAPI".



4. Wählen Sie unter "Produkte ermitteln" die Produkte für den Fernzugriff aus, nach denen Sie suchen wollen.

5 Geben Sie auf der Registerkarte "TAPI" den Telefonnummernbereich ein, den Sie durchsuchen wollen.

- Wenn die Landeskennung mit gewählt wird, müssen Sie das Kontrollkästchen "Landeskennung verwenden" aktivieren und die zu verwendende Landeskennung eingeben.
- Wenn die Option für die Landeskennung nicht aktiviert wurde, ist das Feld abgeblendet. Geben Sie die Ortskennzahl für den zu wählenden Telefonnummernbereich ein. Geben Sie in das Feld "Von Nummer" die Startnummer ein, die gewählt werden soll. Geben Sie in das Feld "Bis Nummer" die letzte Nummer ein.



6 Klicken Sie auf "OK", um den Befehl in die Prüfdatei einzufügen.

CAPI-Prüfeinstellungen konfigurieren

Um nach Produkten für den Fernzugriff zu suchen, die eine CAPI-Verbindung verwenden, müssen Sie einen CAPI-Befehl in Ihre Prüfdatei einfügen.

Symantec ist nicht für Telefongebühren verantwortlich, die möglicherweise während einer Remote Access Perimeter Scanner-Prüfung anfallen.

So konfigurieren Sie CAPI-Prüfeinstellungen:

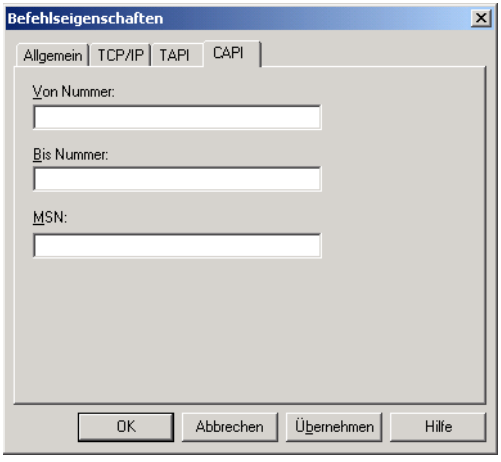
1 Öffnen Sie die Prüfdatei, die Sie anpassen wollen, oder erstellen Sie eine neue Prüfdatei.

2 Klicken Sie im Remote Access Perimeter Scanner-Menü "Befehl" auf "Neu".

3 Klicken Sie im Befehlseigenschaftenfenster auf der Registerkarte "Allgemein" unter "Verbindungstyp" auf "CAPI".

4 Wählen Sie unter "Produkte ermitteln" die Produkte aus, nach denen Sie suchen wollen.

5 Geben Sie auf der Registerkarte "CAPI" die Start- und Endnummern in die Felder "Von Nummer" bzw. "Bis Nummer" ein.



6 Geben Sie in das MSN-Feld Ihre lokale Telefonnummer ein.

7 Klicken Sie auf "OK", um den Befehl in die Prüfdatei einzufügen.

Befehle ändern

Sie können einen in die Prüfdatei eingefügten Befehle jederzeit ändern.

So ändern Sie einen Befehl:

1. Öffnen Sie die Prüfdatei, in der sich der zu ändernde Befehl befindet.
2. Doppelklicken Sie auf den Befehl.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf "OK".

Befehle aus einer Prüfdatei löschen

Sie können einen in eine Prüfdatei eingefügten Befehl jederzeit löschen.

So löschen Sie einen Befehl aus einer Prüfdatei:

1. Öffnen Sie die Prüfdatei, in der sich der zu löschende Befehl befindet.
2. Markieren Sie den Befehl, und drücken Sie dann die Entf-Taste.

Ausführen einer Remote Access Perimeter Scanner-Prüfung

Während der Remote Access Perimeter Scanner-Prüfung werden die Prüfungsdaten im Dialogfeld "Prüfergebnisse" angezeigt. Die Ergebnisse werden im lokalen Textprotokoll gespeichert.

Die im Dialogfeld "Prüfergebnisse" aufgeführten Statusinformationen zeigen, wann der Remote Access Perimeter Scanner eine Verbindung startet. Bis die Verbindung hergestellt ist, die Produkte für den Fernzugriff erkannt und diese Informationen an den Remote Access Perimeter Scanner zurückgegeben werden, vergeht einige Zeit. Möglicherweise ändert sich der Status eine Weile lang nicht, während der Remote Access Perimeter Scanner die Informationen verarbeitet.

So führen Sie eine Remote Access Perimeter Scanner-Prüfung aus:

- Klicken Sie im Remote Access Perimeter Scanner-Menü "Datei" auf "Prüfung starten". Sie können auch die **F5**-Taste drücken.

  Im Fenster "Prüfergebnisse" werden Statusinformationen angezeigt.

Anzeigen von Prüfergebnissen

Nach Abschluss der Prüfung wird das Dialogfeld "Prüfergebnisse" angezeigt. Diese Informationen werden auch im lokalen Textprotokoll gespeichert. Die neuesten Daten werden an das Ende der Protokolldatei angefügt. Wenn die Protokolldatei ihre maximal zulässige Größe überschreitet, werden alte Ereignisse zuerst gelöscht.

So zeigen Sie Prüfergebnisse an:

- Klicken Sie im Remote Access Perimeter Scanner-Menü "Ansicht" auf "Textlogbuch".

Index

Symbole

.atf-Dateien 14
.bhf-Dateien 27, 77
.chf-Dateien 26, 76
.cif-Dateien 27, 77
.cqf-Dateien 27
.sid-Dateien 31

A

ACE/Agent *Siehe* SecurID
ACE/Server *Siehe* SecurID
ATF Converter-Programm 14
AWSHIM.EXE 84
Abhängigkeiten, Anzeigen 45
Active Directory-Dienste 128
Admin.bhf-Datei 76
Admin11.chf-Datei 76
Administrative Vorlage 150
Aktualisierungen
    Informationen 12
    von pcAnywhere 9.2x 15
Alias 61
Anmeldeskripts
    Testen 67, 69
    für Novell-Verteilung 67
    für Windows-Verteilung 65
Anruferdateien 27
Aufzeichnen
    Remote Access Perimeter Scanner 164
    SNMP-Traps 85
    auf zentralen Servern 85
Authentifizierung
    Konfigurieren globaler Benutzer 144
    Microsoft Windows-basierte Methoden 143
    Novell-basierte Methoden 145
    Webbasierte Methoden 146
    Zweifaktor 141
    zentral 141
AutoTransfer-Dateien, Konvertieren 14

B

Befehlskonfigurationsdateien *Siehe* Benutzerdefinierte Befehle
Befehlswarteschlangendateien 27
Benutzerdefinierte Befehle
    Hinzufügen zu Paketdefinitionsdateien 45
    Überblick 43
Benutzerdefinierte Installationen *Siehe* Pakete
Benutzerrechte 9

C

CAPI, Prüfen von Anschlüssen 174
Computernamen, Verbindungen einschränken 140

D

DCOM
    Systemanforderungen
        Windows 98/Me 83
        Windows NT/2000/XP 82
    Ändern von Sicherheitseinstellungen 83
    Überblick 82
dcomcnfg.exe-Datei 84
DynIP, benutzerdefiniertes Paket 11

E

Eingeschränkter Benutzer 9
Ereignisprotokollierung 148
    Generieren automatischer Reaktionen 86
    SNMP-Traps 85
    auf zentralen Servern 85
Ermitteln ungeschützter Hosts 157

F

Fernverwaltung 72
Files.ini-Datei 57, 58

G

Generieren
    Pakete 47
    Produktkonfigurationsdateien 23
Gruppenrichtlinien 149

H

Host-Administrator
    AwShim 84
    Hinzufügen von Computern 75
    Hinzufügen von Computern zu Gruppen 75
    Hinzufügen von Konfigurationsgruppen 74
    Hinzufügen von Objekten für die Host-Konfiguration 79
    Hinzufügen zu MMC 74
    Installieren 72
    Senden von Befehlen 80
    Verbindungsobjektvorlagen 76
    Verteilen von Konfigurationsdateien 79
    Verwalten eines Hosts 80
Host-Computer
    Begrenzen der Verbindungen 140
    Herunterfahren 163
    Sichern 139
Host-Objekte
    Hinzufügen zu Paketen 27
    Konfigurieren 76
Host-Sitzung, Schützen 147

I

IP-Adresse, Verbindungen einschränken 140
ISDN-Verbindungen, Prüfen von Anschlüssen 174
Importieren von Produktmodulen 21
Installation
    Benutzerrechte 9
    Systemanforderungen 8
    über vorherige Versionen 11
Installationsdateien *Siehe* Pakete
Installationsoptionen
    Installationspakete 45
    benutzerdefinierte Produkte 36
Integritätsverwaltung 29

K

Konfigurationsdateien
    Hinzufügen zu Paketen 25
    Verteilen 79
Konfigurationsgruppen 74
Konflikte, Anzeigen 45

L

LAN Host-Produkt 10
LDAP-Überblick 118
LiveUpdate 41
Lizenzvereinbarungen
    Remote Access Perimeter Scanner 158
    Symantec Packager 18

M

MIB 86
MMC
    Gruppenrichtlinien-Snap-In 149
    Hinzufügen von Computern 75
    Hinzufügen von Konfigurationsgruppen 74
    Host-Administrator-Snap-In hinzufügen 74
    Verwalten von Richtlinien 154
Management-Adapter 84
Microsoft Management-Konsole *Siehe* MMC
Migration
    Informationen 12
    von AutoTransfer-Dateien 14
    von Konfigurationsdaten 11
    von Paketen 13
    von pcAnywhere 10.x 13, 14
Modemverbindungen, Prüfen von Anschlüssen 173

N

NT-Authentifizierung, globale Benutzer konfigurieren 144
NetWare-Anmeldeskripts
    Testen 69
    zum Verteilen von Paketen 67
Netscape Directory Server 121, 122
Netzwerkverbindungen
    IP-Adresse einschränken 140
    Prüfen
        SPX-Anschlüsse 171
        TCP/IP-Anschlüsse 169

Novell Directory Server 123
Nur Host-Produkt 10
Nur Remote-Produkt 10

O

Optionsgruppen
    Hinzufügen zu Paketen 35
    Überblick 33
    Übernehmen auf lokalem Computer 35

P

PMI-Datei 21
Packager *Siehe* Symantec Packager
Paketdefinitionsdateien
    Generieren 47
    Hinzufügen benutzerdefinierter Befehle 45
    Importieren in SMS 81
    Produktanforderungen anzeigen 45
    Produkte hinzufügen 45
Pakete
    Definition 44
    Einstellen globaler Optionen 33
    Hinzufügen benutzerdefinierter Befehle 43
    Hinzufügen von Konfigurationsdateien 25
    Integritätsprüfung 29
    Konfigurieren von Produkten 22
    Konfigurieren von Produktinstallationseinstellungen 36
    Produktabhängigkeiten 24
    Produkteinstellungen
        Beibehalten 42
        Host-Vorlagen 39
        Installationsverzeichnis 37
        Online-Registrierung 38
        Produktaktualisierungen 41
        Remote-Vorlagen 40
    Testen 48
    Verteilung
        Testen 60
        mit SMS 61
        über das Internet 51
    Zuweisen einer Seriennummer 30
pcAnywhere Express 11
pcAnywhere.adm-Datei 150, 151
pcAnywhere-Tools
    Host-Administrator 72
    Remote Access Perimeter Scanner 158
Produktanforderungen 45
Produktdefinitionsdateien, Generieren 46
Produktkonfigurationsdateien
    Generieren 23
    Hinzufügen zu Paketdefinitionen 45

R

RAPS *Siehe* Remote Access Perimeter Scanner
Readme-Datei 8
Registrierungsschlüssel 28
Remote Access Perimeter Scanner
    Aufzeichnen 164
    Einstellen von SNMP-Traps 165
    Erstellen einer Prüfdatei 167
    Fernzugriffsprodukte 159
    Herunterfahren von Hosts 163
    Hinzufügen von Befehlen 168
    Installieren 160
    Konfigurieren von Einstellungen 162
    Prüfergebnisse anzeigen 177
    Verwendung von der Befehlszeile 162
    Ändern von Befehlen 176
    Öffnen 161
    Überblick 158
Remote-Objekte
    Hinzufügen zu Paketen 26
    Konfigurieren 76
Richtlinien-Management
    Benutzerrechte 149
    Einstellungen 152
    Windows 2000/XP
        Bearbeiten von Richtlinien 154
        Implementierung 149
        Importieren einer administrativen Vorlage 150
    Windows 98/Me/NT4
        Bearbeiten von Richtlinien 155
        Implementierung 149
        Importieren einer administrativen Vorlage 151

S

SMS
    AwShim 84
    Importieren von pcAnywhere-Dateien 81
    MIB 86
    Verteilung von Paketen 61

SNMP-Traps 85, 148, 165
SPX, Prüfen von Anschlüssen 171
SecurID 141
Seriennummer
    Erstellen 31
    Hinzufügen zu Paketen 31
Shim 84
Sicherheitscode
    Erstellen 31
    Hinzufügen zu Paketen 31
Start.htm-Datei 56
Symantec Packager
    Anpassen von Produkten 22
    Importieren von Produktmodulen 21
    Systemanforderungen 18
    für Migrationen und Aktualisierungen verwenden 16
    Übersicht über den Vorgang 19
Symantec pcAnywhere
    Migration und Aktualisierung 12
    Ordner für Konfigurationsdateien 27
Systemanforderungen 8

T

TAPI, Prüfen von Anschlüssen 173
TCP/IP
    Prüfen von Anschlüssen 169
    Zugriff einschränken 140

V

Verbindungsobjektdateien
    Host 27
    Remote 26
Verbindungsobjekte
    Host 39
    Remote 40
Verteilung
    Anpassen der Dateien 56
    Testen 60
    mit Hilfe von NetWare-Anmeldeskripts 67
    mit Hilfe von Windows-Anmeldeskripts 65
    mit SMS 61
    über das Internet 51
Verzeichnisdienste
    Konfigurieren
        Host-Einstellungen 134
        LDAP-Server 120
        Netscape Directory Server 3.1 121
        Netscape Directory Server 4.0 122
        Novell Directory Server 123
        Remote-Einstellungen 135
        Windows Active Directory 128
        pcAnywhere-Einstellungen 133
    LDAP-Überblick 118
Vorlagen, Host-Administrator 76

W

Web-Server
    Konfigurieren 54
    Kopieren der Installationsdateien 53
Webbasierte Authentifizierung 146
Windows Active Directory 128

Lösungen für Service und Unterstützung

Symantec bemüht sich weltweit um ausgezeichnete Serviceleistungen. Unser Ziel ist, Ihnen professionelle Hilfestellung bei der Anwendung unserer Software zu leisten und professionelle Dienste anzubieten – ganz gleich, in welchem Land.

Die Angebote für Service und Unterstützung sind von Land zu Land unterschiedlich.

Wenn Sie Fragen zu den unten beschriebenen Dienstleistungen haben, lesen Sie bitte den Abschnitt "Alle Kontaktinformationen auf einen Blick".

Registrierung und Lizenzierung

Falls für das von Ihnen installierte Produkt eine Registrierung und/oder ein Lizenzschlüssel erforderlich sind, bietet unsere Lizenz- und Registrierungssite unter www.symantec.com/certificate (auf Englisch) eine schnelle und einfache Methode zur Registrierung Ihres Dienstes. Sie können aber auch auf der Site http://www.symantec.com/region/de/techsupp/enterprise das Produkt auswählen, das Sie registrieren möchten, und auf der Produkt-Homepage den Link "Lizenzierung und Registrierung" wählen.

Wenn Sie ein Unterstützungsabonnement erworben haben, können Sie technische Unterstützung über Telefon und Internet in Anspruch nehmen. Halten Sie bei der ersten Kontaktaufnahme entweder die Lizenznummer aus Ihrem Lizenzzertifikat oder die bei der Unterstützungsregistrierung erzeugte Kontakt-ID bereit, so dass ein Mitarbeiter der technischen Unterstützung ihre Berechtigung überprüfen kann. Wenn Sie kein Unterstützungsabonnement erworben haben, erfahren Sie Einzelheiten zum Erwerb technischer Unterstützung über Ihren Händler oder den Symantec-Kundenservice.

Sicherheits-Updates

Aktuelle Informationen zu Viren und Sicherheitsbedrohungen finden Sie auf der Symantec Security Response-Website (vormals Antivirus Research Centre) unter folgender Adresse:

www.symantec.de/region/de/avcenter/index.html

Diese Site enthält umfassende Online-Informationen zu Sicherheits- und Virenbedrohungen sowie die neuesten Virendefinitionen. Virendefinitionen können außerdem mithilfe der LiveUpdate-Funktion Ihres jeweiligen Produkts heruntergeladen werden.

Erneuern des Abonnements für Virendefinitions-Updates

Wenn Sie zusammen mit Ihrem Produkt einen Wartungsvertrag erwerben, sind Sie ein Jahr lang zum Bezug kostenloser Virendefinitionen über das Internet berechtigt. Nach Ablauf Ihres Wartungsvertrags erhalten Sie Informationen zur Erneuerung des Vertrags über Ihren Händler oder den Symantec-Kundenservice.

Symantec-Websites:

Symantec-Homepage (nach Sprache):

Deutsch:	http://www.symantec.de
Englisch:	http://www.symantec.com
Französisch:	http://www.symantec.fr
Italienisch:	http://www.symantec.it
Niederländisch:	http:// www.symantec.nl
Portugiesisch:	http://www.symantec.com/br
Spanisch:	http://www.symantec.com/region/es http://www.symantec.com/mx

Symantec Security Response:

www.symantec.de/region/de/avcenter/index.html

Service und Unterstützung für Symantec Enterprise:

http://www.symantec.com/region/de/techsupp/enterprise/

Produktspezifisches Newsbulletin:

USA, Asien-Pazifik/Englisch:

http://www.symantec.com/techsupp/bulletin/index.html

Europa, Nahost und Afrika/Englisch:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

Deutsch:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

Französisch:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html.

Italienisch:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Niederländisch:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

Lateinamerika

Spanisch:

http://www.symantec.com/region/mx/techsupp/bulletin/index.html

Portugiesisch:

http://www.symantec.com/region/br/techsupp/bulletin/index.html

Technische Unterstützung

Als Teil von Symantec Security Response verfügt unser globales Team für die technische Unterstützung weltweit über Support-Zentren. Vorrangige Aufgabe ist die Beantwortung von Fragen zu Produktfunktionen, zur Installation und zur Konfiguration sowie die Bereitstellung von aktuellen Informationen in unserer webbasierten Unterstützungsdatenbank. Dabei arbeiten wir eng mit anderen Unternehmensbereichen von Symantec zusammen, um Ihre Fragen schnellstmöglich zu beantworten. In enger Kooperation mit den Product Engineering- und Security Research Center-Experten bieten wir Ihnen umfassende Warndienste und Virendefinitions-Updates für Virenausbrüche und Sicherheitswarnungen. Unser Angebot umfasst u. a.:

- Zahlreiche Unterstützungsoptionen, mit denen Sie den Umfang des für Ihre Unternehmensgröße benötigten Supports flexibel wählen können.
- Telefon- und Internetunterstützung, über die Sie schnelle Hilfe und aktuelle Informationen erhalten.
- Produkt-Updates gewährleisten automatischen Schutz durch Software-Upgrades.
- Inhalts-Updates für Virendefinitionen und Sicherheits-Signaturen sorgen für optimalen Schutz.
- Der globale Support durch die Experten von Symantec Security Response steht Ihnen weltweit rund um die Uhr (24x7) in zahlreichen Sprachen zur Verfügung.
- Erweiterte Funktionen wie beispielsweise der Symantec Alerting Service und der persönliche Technical Account Manager gewährleisten verbesserte Reaktionszeiten und proaktiven Sicherheits-Support.

Aktuelle Informationen über unsere Unterstützungsprogramme finden Sie auf unserer Website.

Kontakt

Kunden mit einem gültigen Unterstützungsvertrag können sich telefonisch oder über das Internet an die technische Unterstützung wenden, entweder unter der nachstehenden URL oder über die weiter hinten in diesem Dokument aufgeführten regionalen Unterstützungssites.

www.symantec.com/region/de/techsupp/enterprise/

Halten Sie dabei die folgenden Informationen bereit:

- Nummer des Produkt-Release
- Hardware-Informationen
- Verfügbarer Arbeitsspeicher, freier Festplattenspeicher, installierte Netzwerkkarte
- Betriebssystem
- Versions- und Patch-Nummer
- Netzwerktopologie
- Router, Gateway und IP-Adressinformationen
- Beschreibung des Problems
- Fehlermeldungen/Protokolldateien
- Die vor der Kontaktaufnahme mit Symantec durchgeführten Schritte zur Problemlösung
- Kürzlich durchgeführte Änderungen der Software- und/oder Netzwerkkonfiguration

Kundenservice

Das Symantec-Kundenservice-Center hilft Ihnen bei nicht-technischen Anfragen, beispielsweise:

- Allgemeine Produktinformationen (z. B. Leistungsmerkmale, Preise, Sprachverfügbarkeit, Händler in Ihrer Nähe usw.)
- Hilfe bei einfachen Problemen, z. B. wie Sie Ihre Versionsnummer überprüfen können
- Neueste Informationen zu Produkt-Updates und -Upgrades
- Wie Sie Ihr Produkt aktualisieren oder eine neue Version (Upgrade) installieren können
- Wie Sie Ihr Produkt und/oder Lizenzen registrieren können
- Informationen zu den Lizenzprogrammen von Symantec
- Informationen zu Upgrade-Versicherung und Wartungsverträgen
- Ersatz fehlender CDs und Handbücher
- Aktualisierung Ihrer Registrierungsdaten bei Adress- und Namensänderungen
- Beratung zu den Optionen der technischen Unterstützung von Symantec

Ausführliche Kundenservice-Informationen erhalten Sie auf der Symantec-Website für Service und Unterstützung oder durch einen Anruf beim Kundenservice-Center von Symantec. Die Webadressen und die Nummer Ihres lokalen Kundenservice-Centers finden Sie unter "Alle Kontaktinformationen auf einen Blick".

Alle Kontaktinformationen auf einen Blick

Europa, Naher Osten und Lateinamerika

Symantec-Websites für Service und Unterstützung

Deutsch:	www.symantec.de/desupport/
Englisch:	www.symantec.com/eusupport/
Französisch:	www.symantec.fr/frsupport
Italienisch:	www.symantec.it/itsupport/
Niederländisch:	www.symantec.nl/nlsupport/
Portugiesisch:	www.symantec.com/region/br/techsupp/
Spanisch:	www.symantec.com/region/mx/techsupp/
Symantec FTP: (Herunterladen von technischen Hinweisen und neuesten Patches)	ftp.symantec.com

Besuchen Sie "Symantec Service und Unterstützung" im Internet. Dort finden Sie technische und allgemeine Informationen zu Ihrem Produkt.

Symantec Security Response:

www.symantec.de/region/de/avcenter/index.html

Produktspezifisches Newsbulletin:

USA/Englisch:

http://www.symantec.com/techsupp/bulletin/index.html

Europa, Nahost und Afrika/Englisch:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

Deutsch:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

Französisch:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

Italienisch:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Niederländisch:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

Spanisch:

http://www.symantec.com/region/mx/techsupp/bulletin/index.html

Portugiesisch:

http://www.symantec.com/region/br/techsupp/bulletin/index.html

Symantec-Kundenservice

Bietet allgemeine Produktinformationen und Beratung per Telefon in den folgenden Sprachen: Englisch, Deutsch, Französisch und Italienisch.

Belgien	+ (32) 2 2750173
Dänemark	+ (45) 35 44 57 04
Deutschland	+ (49) 69 6641 0315
Finnland	+ (358) 9 22 906003
Frankreich	+ (33) 1 70 20 00 00
Großbritannien	+ (44) 20 7744 0367
Irland	+ (353) 1 811 8093
Italien	+ (39) 02 48270040
Luxemburg	+ (352) 29 84 79 50 30
Niederlande	+ (31) 20 5040698
Norwegen	+ (47) 23 05 33 05
Österreich	+ (43) 1 50 137 5030
Schweden	+ (46) 8 579 29007
Schweiz	+ (41) 2 23110001
Spanien	+ (34) 91 7456467
Südafrika	+ (27) 11 797 6639
Andere Länder	+ (353) 1 811 8093
(Nur in englischer Sprache)	

Symantec-Kundenservice - Korrespondenzadresse

Symantec Ltd
Customer Service Centre
Europe, Middle East and Africa (EMEA)
PO Box 5689
Dublin 15
Irland

Für Lateinamerika

Symantec bietet weltweit technische Unterstützung und Kundenservice. Die Dienstleistungen sind von Land zu Land unterschiedlich und umfassen internationale Partner in Regionen, in denen keine Symantec-Geschäftsstelle vorhanden ist. Bitte wenden Sie sich für allgemeine Informationen an die Symantec-Geschäftsstelle für Service und Unterstützung in Ihrer Region.

Argentinien

Pte. Roque Saenz Peña 832 - Piso 6
C1035AAQ, Ciudad de Buenos Aires
Argentinien

Hauptrufnummer	+54 (11) 5811-3225
Website	http://www.service.symantec.com/mx
Gold Support:	0800-333-0306

Venezuela

Avenida Francisco de Miranda. Centro Lido
Torre D. Piso 4, Oficina 40
Urbanización el Rosal
1050, Caracas D.F.
Venezuela

Hauptrufnummer	+58 (212) 905-6327
Website	http://www.service.symantec.com/mx
Gold Support:	0800-1-00-2543

Columbien

Carrera 18# 86A-14
Oficina 407, Bogota D.C.
Columbien

Hauptrufnummer	+57 (1) 638-6192
Website	http://www.service.symantec.com/mx
Gold Support:	980-915-5241

Brasilien

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasilien, SA

Hauptrufnummer	+55 (11) 5189-6300
Fax:	+55 (11) 5189-6210
Website	http://www.service.symantec.com/br
Gold Support:	000814-550-4172

Chile

Alfredo Barros Errazuriz 1954
Oficina 1403
Providencia,
Santiago de Chile
Chile

Hauptrufnummer	+56 (2) 378-7480
Website	http://www.service.symantec.com/mx
Gold Support:	0800-333-0306

Mexiko

Boulevard Adolfo Ruiz Cortines 3642 Piso 8,
Colonia Jardines del Pedregal,
01900, Mexico D.F.
Mexiko

Hauptrufnummer	+52 (55) 5481-2600
Website	http://www.service.symantec.com/mx
Gold Support:	001880-232-4615

Übriges Latinamerika

9155 South Dadeland Blvd.
Suite 1100,
Miami, FL 33156
U.S.A

Website	http://www.service.symantec.com/mx	
Gold Support:	Costa Rica	800-242-9445
	Panama	800-234-4856
	Puerto Rico	800-232-4615

Für Asien-Pazifik

Symantec bietet weltweit technische Unterstützung und Kundenservice. Die Dienstleistungen sind von Land zu Land unterschiedlich und umfassen internationale Partner in Regionen, in denen keine Symantec-Geschäftsstelle vorhanden ist. Bitte wenden Sie sich für allgemeine Informationen an die Symantec-Geschäftsstelle für Service und Unterstützung in Ihrer Region.

Geschäftsstellen für Service und Unterstützung

AUSTRALIEN

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Australien

Hauptrufnummer	+61 2 8879 1000
Fax	+61 2 8879 1001
Website	http://service.symantec.com

Gold Support	1800 805 834	gold.au@symantec.com
Support Contracts Admin	1800 808 089	contractsadmin@symantec.com

CHINA

Symantec China
Unit 1-4, Level 11
Tower E3, The Towers, Oriental Plaza
No.1 East Chang An Ave.,
Dong Cheng District
Beijing 100738
China P.R.C.

Hauptrufnummer	+86 10 8518 3338
Technische Unterstützung	+86 10 8518 6923
Fax	+86 10 8518 6928
Website	http://www.symantec.com.cn

HONGKONG

Symantec Hong Kong
Central Plaza
Suite #3006
30th Floor, 18 Harbour Road
Wanchai
Hongkong

Hauptrufnummer	+852 2528 6206
Technische Unterstützung	+852 2528 6206
Fax	+852 2526 2646
Website	http://www.symantec.com.hk

INDIEN

Symantec India
Suite #801
Senteck Centrako
MMTC Building
Bandra Kurla Complex
Bandra (East)
Mumbai 400051, Indien

Hauptrufnummer	+91 22 652 0658
Fax	+91 22 652 0671
Website	http://www.symantec.com/india
Technische Unterstützung:	+91 22 657 0669

KOREA

Symantec Korea
15,16th Floor
Dukmyung B/D
170-9 Samsung-Dong
KangNam-Gu
Seoul 135-741
Südkorea

Hauptrufnummer	+822 3420 8600
Fax	+822 3452 1610
Technische Unterstützung	+822 3420 8650
Website	http://www.symantec.co.kr

MALAYSIA

Symantec Corporation (Malaysia) Sdn Bhd
31-3A Jalan SS23/15
Taman S.E.A.
47400 Petaling Jaya
Selangor Darul Ehsan
Malaysia

Hauptrufnummer	+603 7805 4910
Fax	+603 7804 9280
Enterprise E-Mail	gold.apac@symantec.com
Enterprise gebührenfrei	+1800 805 104
Website	http://www.symantec.com.my

NEUSEELAND

Symantec New Zealand
Level 5, University of Otago Building
385 Queen Street
Auckland Central 1001
Neuseeland

Hauptrufnummer	+64 9,375 4100	
Fax	+64 9 375 4101	
Website für Unterstützung	http://service.symantec.co.nz	
Gold Support	0800 174 045	gold.nz@symantec.com
Support Contracts Admin	0800 445 450	contractsadmin@symantec.com

SINGAPUR

Symantec Singapore
3 Phillip Street
#17-00 & #19-00 Commerce Point
Singapur 048693

Hauptrufnummer	+65 6239 2000
Fax	+65 6239 2001
Technische Unterstützung	+65 6239 2099
Website	http://www.symantec.com.sg

TAIWAN

Symantec Taiwan
2F-7, No.188 Sec.5
Nanjing E. Rd.,
105 Taipei
Taiwan

Hauptrufnummer	+886 2 8761 5800
Corporate Support	+886 2 8761 5800
Fax	+886 2 2742 2838
Website	http://www.symantec.com.tw

Wir haben uns um größtmögliche Genauigkeit der Informationen in diesem Dokument bemüht. Die Informationen unterliegen jedoch gelegentlichen Änderungen. Symantec Corporation behält sich das Recht vor, solche Änderungen ohne vorherige Ankündigung vorzunehmen.